HAAGA-HELIA
ammattikorkeakoulu

Tietoturvaopas PK-yritykselle

Henry Kokko

Opinnäytetyö
Tietojenkäsittelyn koulutusohjelma
2014

HAAGA-HELIA ammattikorkeakoulu

Koulutusohjelma

Tiivistelmä

30.4.2014

Tekijä Henry Kokko	**Aloitusvuosi** 2010
Opinnäytetyön nimi Tietoturvaopas PK-yritykselle	**Sivu- ja liitesivumäärä** 39 + 2
Opettajat tai ohjaajat Juhani Merilinna	

Tietoturva on aiheuttanut PK-yrityksille paljon päänvaivaa huonon tietämyksen, heikon rahatilanteen tai muun syyn vuoksi. Tämä opinnäytetyö on suunniteltu pienille ja keskisuurille yrityksille tietoturvaoppaaksi. Oppaan tavoitteena on parantaa kyseisten yritysten tietoturvaa, jotta he pystyvät suojautumaan hakkereita, krakkereita ja muita hyökkääjiä vastaan.

Oppaassa käydään läpi tunnetuimmat haittaohjelmat ja minkälaisia haittoja ne voivat aiheuttaa yritykselle. Sisältö on rajoitettu täyttämään vain pienten ja keskisuurten yritysten tarpeet.

Yritysten resurssit voidaan jakaa neljään eri ryhmään: Laitteistot, ohjelmistot, tiedo ja henkilökunta. Jokaiselle ryhmälle on oma lukunsa, joissa kerrotaan tarkemmin kyseisten ryhmien aiheuttamista tietoturvauhista. Tämän oppaan lukemalla työnantajat pystyvät varautumaan oppaassa esitettyjä uhkia vastaan.

Hyökkääjät työskentelevät erilaisin tavoin, joten on tärkeää tietää heidän käyttäytymismalleista ja hyökkäystavoista, jotta voidaan varautua parhaalla mahdollisella tavalla hyökkäysten sattuessa.

Useat työnantajat pitävät omia työntekijöitään suurimpana tietoturvauhkana, joten oppaaseen on myös sisällytetty selkeät ohjeet henkilökuntaa varten.

Oppaassa on helposti ymmärrettävät ohjeet viruksentorjuntaohjelmiston ja palomuurin käyttöönottoa varten. Lopuksi löytyy tietoturvakysely, josta työnantaja pystyy saamaan jonkinlaista kuvan yrityksen tietoturvan tilasta.

Asiasanat
Tietoturva, PK-yritys, palomuuri, haittaohjelmat, virustorjunta, virus

HAAGA-HELIA ammattikorkeakoulu

Koulutusohjelma

Tiivistelmä

30.4.2014

Author Henry Kokko	**Year of entry** 2010
The title of thesis IT security guide for small and medium business	**Number of report pages and attachment pages** 39 + 2
Advisor Juhani Merilinna	

For small and medium enterprises, information security has been increasingly difficult to deal with due to the lack of knowledge or poor financial situation amongst many other reasons. This thesis was designed for small and medium enterprises as an information security guide. Its goal is to improve companies' information security so they will be able to preserve their systems against hackers, crackers and other forms of attacks.

This guide covers the behavior of most known malware programs and what type of damage they can cause to a company. Its content is limited to fulfill the needs of small and medium enterprises.

A company's resources can be divided into four different categories: hardware, software, data and personnel. The thesis discusses these concepts, including the types of threats directed at companies via these mediums. By reading this guide, employers can learn about the types of protection available to cover these areas.

Attackers work in a variety of ways so it is prudent to be armed with knowledge of their behavior and their methods of attack in preparation of these events.

As many employers believe that the personnel are often the weakest link with regard to security, detailed guidelines for staff were included in this guide.

The guide has easily understandable instructions regarding antivirus and firewall software. In addition, there is an information security questionnaire so an employer can ascertain the current condition of information security within the company.

Keywords
Information Security, small and medium enterprises, firewall, malware, antivirus-software, virus

Sisällys

1 Johdanto

Tietoturva on yksi tärkeimmistä asioita, joita tulisi ottaa huomioon kun yrityksen tietojärjestelmiä suunnitellaan. PK-yritysten tietoturva on ollut pitkään huolenaiheena Hyvin turvattu järjestelmä nopeuttaa työntekoa ja säästää työtunteja sekä muita yrityksen resursseja. Kun puhutaan tietoturvasta, niin usein uskotaan, että viruksentorjuntaohjelmisto ja palomuuri tuovat riittävän suojan. Tämä voi pitää paikkansa peruskäyttäjällä, mutta yritystoiminnassa on otettava paljon muitakin asioita huomioon, kuten esimerkiksi varmuuskopiointi, tietojen, ohjelmistojen ja laitteistojen suojaaminen sekä hyökkäyksiltä suojautuminen.

Yrityksiin kohdistuvat tietoturvariskit ovat suurempia, sillä erilaiset organisaatiot ovat kiinnostuneet yritysten tiedoista eri syistä johtuen. Yrityksiin kohdistuvat haitat eivät aina tule yrityksen ulkopuolelta, vaan yrityksen omat työntekijät voivat saada paljon tuhoa aikaan tahallisesti tai tahattomasti huonon perehdytyksen tai muiden syiden vuoksi.

Oppaassa käydään läpi yleisimmät haittaohjelmat ja hyökkäystavat, jotta yrityksessä ymmärretään minkälaisia uhkia on olemassa. Tämän jälkeen oppaassa kerrotaan suojattavista resursseista, josta yritykselle saadaan ideoita, että mitä resursseja suojataan ja miten. Hyökkäyksien torjumisesta kerrottavassa kappaleessa käydään läpi, kuinka suojautua hyökkäyksiltä ja minkälaisia ovat tyypillisimmät hyökkääjät. Henkilökunnan perehdyttämisestä kerrottavassa kappaleessa on ohjeet, kuinka työskennellä tietoturvallisesti ja miksi. Lopuksi oppaassa on ohjeet Comodo Firewall palomuurin ja Avira Antivirus viruksentorjuntaohjelmiston käyttöönottoon.

Työn tavoitteena on saada tehtyä helposti lähestyttävä tietoturvaopas pienille ja keskisuurille yrityksille, sillä PK-yritysten tietoturva on aiheuttanut paljon ongelmia yrityksille. Oppaan avulla saadaan yleistä tietoutta tietoturvasta, varautumisohjeita ja erilaisia neuvoja, kuinka toimia erilaisissa tilanteissa. Tiedonhakumenetelmänä on käytetty kvalitatiivista menetelmää. Lähteinä on käytetty ainoastaan luotettavia lähteitä, kuten tietoturva-alan ammattilaisia, tietoturvayrityksiä, laitevalmistajia ja sekä ohjelmistoalan yrityksiä.

2 Käsitteiden määrittely

Opinnäytetyössä käytetään käsitteitä, joita ei välttämättä ole itsestään selviä. Tästä syystä seuraavaksi täsmennetään, että mitä oppaassa käytetyt asiasanat tarkoittavat.

Järjestelmänvalvoja

Käyttäjätunnus, jolla on kaikki oikeudet. Yleensä ylläpitäjien käytössä oleva käyttäjätunnus.

Reititin

Reititin on laite, joka ohjaa verkon tietoliikennepaketit oikeaan osoitteeseen.

IP-osoite

IP-osoite on osoite, joka yksilöi laitteen verkossa. Jokaisella verkossa toimivalla laitteella on oma IP-osoitteensa, että verkon liikennettä pystytään ohjaamaan halutulle laitteelle. IP-osoite on yleensä pistenotaatiomuodossa, kuten esimerkiksi 180.128.10.210. Osoite on jaettu neljään lukuun, jotta ihmiset muistaisivat sen helpommin. Jokainen luku voi olla väliltä 0-255.

IP-paketti

IP-paketti sisältää erilaisia tietoja, kuten mistä paketti on tullut, mihin se on menossa ja varsinaisen datan, mitä halutaan siirtää. Kaikki tieto verkossa liikkuu IP-pakettien sisällä.

Portti

Portit määrittelevät liikenteen tyypin. Portin numero kertoo millaista liikennettä se päästää lävitseen. Esimerkiksi portti numero 80 päästää http liikennettä lävitseen, kun taas portti numero 20 on FTP liikennettä varten.

3 Haittaohjelmat

Haittaohjelmia ovat sellaiset ohjelmat, joiden tekijät yrittävät saada jonkinlaista ikävää aikaiseksi uhrin koneella. Yleensä haittaohjelmilla yritetään saada jonkinlaista hyötyä, oli se sitten mainetta tai taloudellista hyötyä. Tämä onnistuu esimerkiksi varastamalla käyttäjän luottokorttitietoja tai pankkitunnuksia. Haittaohjelmia on erilaisia ja yleisimmistä niistä on tarkennuksia alla olevissa alaotsikoissa.

3.1 Virukset

Yksinkertaistettuna virukset ovat tietokoneohjelmia, jotka käynnistyessään yrittävät levittäytyä mahdollisimman laajalle kopioimalla itseään muihin tietokoneen ohjelmiin ja tiedostoihin. Jotkut virukset voivat myös kopioitua reitittimen kiintolevylle ja aiheuttaa tällä tavoin vahinkoa.

Ne voivat tehdä mitä tahansa mitä muutkin tietokoneen ohjelmat ja yleensä virukset ovat tehty aiheuttamaan haittaa käyttäjälle erilaisilla tavoilla. Virukset voivat yrittää varastaa käyttäjän tietoja tai viruksen tekijä pystyy käyttämään saastunutta konetta erilaisiin hyökkäyksiin.

Virukset vaativat käyttäjältä jonkinlaista toimenpidettä toimiakseen, kuten liitetiedoston avaamisen sähköpostista. Virukset voivat levitä muun muassa sähköpostitse ja erilaisten tallennusmedioiden välityksellä. Microsoftin Windows-käyttöjärjestelmien suuresta suosiosta johtuen suurin osa viruksista on tehty Windows-käyttöjärjestelmille. (United States Computer Emergency Readiness Team; Katherine Noyes 2010; Symantec a,)

3.2 Madot (Worms)

Madot eroavat viruksista siten, että ne eivät vaadi minkäänlaisia toimenpiteitä toimiakseen. Ne käyttävät ohjelmien tietoturva-aukkoja toimiakseen. Niitä löytyy yleensä päivittämättömistä ohjelmista. Madot etsivät tietokoneelta sähköpostiosoitteita, joihin ne lähettävät saastuneita sähköpostiviestejä. Mato muuttaa lähettäjän tietoja, jolloin se näyttäisi tulevan tutuilta henkilöiltä. Toisin kuin virukset, madot eivät aina

aiheuta vahinkoja koneelle, mutta yleensä hidastavat tietokonetta ja verkkoa. (Symantec b.)

3.3 Troijalaiset (Trojans)

Troijalaiset ovat haittaohjelmia, jotka yleensä naamioituvat tiedostoiksi tai ohjelmiksi, joita käyttäjä voisi haluta käyttää. Ne voivat tehdä erilaisia haittoja koneelle, kuten avata portin, jota kautta voidaan ottaa etäyhteys saastuneeseen koneeseen. Troijalaiset pystyvät myös lataamaan lisää haittaohjelmia koneelle tai yrittävät päästä käsiksi koneella oleviin tietoihin. (Symantec c.)

3.4 Takaovet (Backdoors)

Takaovi on ylläpitoväline, jolla päästään käsiksi ohjelman koodiin. Se on tehty, jotta kehittäjä pääsee testaamaan ohjelmaa tai korjaamaan ohjelman virheitä kehitysvaiheessa. Näiden välineiden tarkoitus on olla ohjelman ylläpitäminen, mutta hyökkääjät käyttävät niitä usein, sillä niillä pääsee läpi kaikista ohjelman suojausmekanismeista. Takaovet voivat aiheuttaa ongelmia, sillä hyökkääjä pystyy saamaan yhteyden auki uhrin koneelle ja aiheuttamaan erilaisia haittoja, kuten lähettämään ja vastaanottamaan sähköpostia, saamaan tietokoneen tietoja haltuunsa, selailemaan kovalevyjen sisältöä ja vaihtamaan aika asetuksia. (F-secure.)

3.5 Ohjelmien tietoturva-aukkojen hyväksikäyttäjät (Exploits)

Ohjelmien tietoturva-aukkoja hyväksikäyttävät haittaohjelmat voivat pahimmillaan antaa hyökkääjälle mahdollisuuden siirtää käyttäjän tietokoneelle haitallista koodia. Kolme yleisintä hyväksikäytölle altista tiedostotyyppiä ovat Java, HTML/JavaScript ja erilaiset dokumentit, kuten PDF- ja Word -dokumentit. Kyseisten haittojen estäminen on suhteellisen helppoa, sillä ohjelmistojen päivittäminen ja ajantasalla pitäminen riittää pitämään tietoturvan kunnossa päivitettyjen ohjelmien osalta. (Microsoft.)

3.6 Mainosohjelmat (adware)

Mainosohjelmat tuovat käyttäjän näkyviin pop-up mainosikkunoita. Jotkut mainosohjelmista muuttavat aloitussivun joksikin muuksi ja voivat lisätä työkalupalkkeja internetselaimeen. Jos mainosohjelma on tullut jonkin ohjelman mukana, kyseinen ohjelma ei välttämättä enää toimi mainosohjelman poiston jälkeen. Jotkut mainosohjelmista keräävät tietoja käyttäjästä ja lähettävät niitä kolmansille osapuolille.

Paras puolustus mainosohjelmilta suojautumiseen on lukea ohjelmaa asentaessa sopimusehdot. Ilmaisohjelmien mukana tulevat mainosohjelmat ovat yleensä ohjelman hinta. Joidenkin ohjelmien mainosohjelmia ei kuitenkaan ole pakko asentaa, joten on hyvä olla tarkkana ohjelmien asennuksen aikana. Jos ohjelmaa ei pystytä asentamaan ilman mainosohjelmia, niin kyseistä ohjelmaa ei välttämättä kannata käyttää. (Mary Landesman.)

3.7 Rootkitit

Rootkitit ovat haittaohjelmia, jotka antavat hyökkääjälle järjestelmänvalvojan tasoiset käyttöoikeudet kohteen käyttöjärjestelmään. Aluksi rootkit asennetaan tietokoneeseen peruskäyttäjän oikeuksilla, josta ne erilaisten tietoturva-aukkojen tai salasanan murtamisen avulla saavat kaikki oikeudet. Rootkitit antavat hyökkääjälle mahdollisuuden asentaa lisää haittaohjelmia käyttöjärjestelmään, kuten verkkoliikennettä seuraavia tai näppäimistön painalluksia tallentavia ohjelmia. (Margaret Rouse 2008.)

4 Hyökkäykset

Kaikki hyökkäykset eivät käytä pelkästään haittaohjelmia, vaan niiden lisäksi on myös muita hyökkäystapoja. Näitä hyökkäyksiä ei pysty torjumaan viruksentorjuntaohjelmistolla, vaan käyttäjältä vaaditaan erilaisia toimenpiteitä hyökkäyksiltä suojautumiseen.

4.1 Salakuuntelu

Suurin osa verkkoliikenteestä kulkee salaamattomana, joten hyökkääjä voi päästä käsiksi tietoihin esimerkiksi suojaamattoman langattoman verkon kautta. Salakuuntelu on suurin tietoturvauhka, mitä yrityksessä joudutaan kohtaamaan. Ilman vahvaa salausta ulkopuoliset pystyvät tarkastelemaan verkkoliikenteen sisältöä.

4.2 Tietojen muokkaus

Erilaisia tietoja lähetettäessä täytyy olla varma, ettei niitä muuteta matkan aikana. Hyökkääjät voivat tiedot saadessaan muokata niitä ja lähettää ne eteenpäin niin, ettei vastaanottaja välttämättä tiedä, että tietoja on muutettu. Tietoja pystytään muuttamaan myös muun muassa nettikaupoissa, jolloin ostotilanteessa on tärkeää, että tuotteiden määrät, tiedot tai hinnat eivät muutu ostaessa tai myytäessä tuotteita.

4.3 Identiteetin huijaus (Identity Spoofing)

Useimmat verkot ja käyttöjärjestelmät käyttävät IP-osoitteita tunnistaakseen toisen osapuolen. Joissakin tapauksissa on mahdollista muuttaa IP-osoitetta siten, että saadaan yhteys haluttuun kohteeseen. Joissakin tapauksissa hyökkääjä käyttää ohjelmia, jotka muuttavat IP-pakettien tietoja siten, että yhteys näyttäisi tulevan yrityksen sisäverkosta. Yhteyden saamisen jälkeen hyökkääjä voi poistaa tietoja, lisätä haittaohjelmia yrityksen laitteisiin tai hyökätä toisilla tavoin sisään päästessään.

4.4 Mies välissä -hyökkäys (Man-in-the-Middle Attack)

Tällainen hyökkäys onnistuu niin, että ulkopuolinen henkilö tarkastelee aktiivisesti, tallentaa tai kontrolloi kahden osapuolen välistä verkkoliikenteen sisältöä. Hyökkääjä yrittää saada molemmat osapuolet uskomaan, että heidän välinen liikenne on vain heidän kahden nähtävillä, vaikka todellisuudessa kaikki liikenne kulkee hyökkääjän kautta.

4.5 Salasanan murtamiset

Käyttöjärjestelmän oikeudet ja verkon resurssit on määritelty käyttäjätunnuksen perusteella. Kun hyökkääjä löytää sopivan käyttäjätunnuksen, niin salasanan saatuaan hän saa samat oikeudet, kuin käyttäjätunnuksen oikea omistaja. Jos hyökkääjä saa ylläpitäjän oikeudet, hän voi tehdä itselleen myöhempää käyttöä varten käyttäjätunnuksia, joissa on täydet oikeudet. Vanhemmat ohjelmat eivät aina salaa tietoja käyttäjästä, kun kirjaudutaan verkon kautta, joten salakuuntelijat pystyvät keräämään käyttäjän tiedot ja salasanan sitä kautta.

Hyökkääjä pystyy verkon käyttöoikeudet saadessaan poistamaan, ohjaamaan muualle tai muokkaamaan tiedostojen sisältöä, saamaan tietoa yrityksen tietokoneista, verkoista ja käyttäjistä ja muuttamaan verkon asetuksia, kuten esimerkiksi käyttöoikeuksia.

4.6 Denial-of-service hyökkäys (DDOS)

DDOS -hyökkäyksillä estetään verkon käyttö normaaleilta käyttäjiltä. Hyökkääjä lähettää paljon liikennettä verkon kautta niin kauan, että palvelin saadaan kaadettua ylikuormituksen vuoksi. Hyökkääjä voi myös lähettää vääränlaista tietoa ohjelmille, mikä johtaa ohjelmien epätavalliseen toimintaan tai ohjelmien sulkemiseen.

4.7 Sovelluskerroshyökkäys (Application-layer attack)

Sovelluskerroshyökkäyksellä hyökätään sovelluspalvelimiin aiheuttamalla virhe palvelimen käyttöjärjestelmään tai ohjelmiin. Tämän tuloksena hyökkääjä pääsee käyttöoikeuksien määrittelijän lävitse, jolloin hyökkääjä voi:

- Lukea, lisätä, poistaa tai muokata tiedostoja tai tehdä haittaa käyttöjärjestelmälle.
- Lisätä viruksen joka leviää tietokoneiden ja ohjelmien kautta verkkoon.
- Lisätä haisteluohjelman, joka kerää tietoja yrityksen verkosta, joiden avulla pystytään myöhemmin kaatamaan laitteistot ja verkko
- Sulkea ohjelmia tai käyttöjärjestelmiä
- Ottaa järjestelmää suojaavia asetuksia tai ohjelmia pois käytöstä myöhempiä hyökkäyksiä varten.

4.8 Salasananhaisteluhyökkäys

Salasanan haistelija tai snifferi on ohjelma, joka pystyy lukemaan ja tallentamaan verkon muutoksia ja lukemaan verkossa lähetettyjen pakettien sisältöä. Jos paketit eivät ole salattuja, niin salasanan haistelija pystyy näyttämään paketin täyden sisällön. Hyökkääjä saa salasanan haistelijalla tietoa yrityksen verkosta, jonka avulla hän pystyy kaatamaan kyseisen verkon.

4.9 Verkkourkinta (Phishing)

Verkkourkinnassa yritetään huijata käyttäjää antamaan hyökkääjää kiinnostavia tietoja, kuten luottokorttitietoja tai salasanoja. Uhri yritetään ohjata hyökkääjän tekemälle sivustolle, jonka ulkoasu näyttää jonkin olemassa olevan yrityksen sivuilta. Tämä onnistuu lähettämällä uhrille sähköpostia, joka sisältää linkit kyseisille sivuille.

Lähettäjän nimi on muutettu halutun yrityksen nimeksi ja käyttäjälle uskotellaan, että heidän täytyy kirjautua yrityksen sivuilla sisään. Uhrin yrittäessä kirjautua sisään hyökkääjä saa uhrin kirjautumistiedot, jolloin he pääsevät käsiksi uhrin käyttäjätunnukseen.

Sähköposteissa olevat linkit ovat muutettu näyttämään siltä, kuin ne ohjaisivat uhrin haluamalle sivulle. Todellisen osoitteen näkee, kun vie osoittimen linkin päälle ja tarkastaa selaimen linkkien esikatselukohdasta todellisen osoitteen.

5 Suojattavat resurssit

Yleensä yrityksessä oleva omaisuus pystytään jakamaan neljään ryhmään:

- Laitteistot - Työasemat, oheislaitteet, komponentit, mobiililaitteet
- Ohjelmistot - Käyttöjärjestelmät, käytettävät ohjelmat
- Data - Tiedot ja tietokannat
- Henkilökunta

Laitteistot ja ohjelmistot ovat helppoja korvata, jos yrityksellä on varallisuutta, mutta yrityksen omat ohjelmistot ja tiedot voivat olla korvaamattomia. Rajallisten varojen puitteissa on kuitenkin priorisoitava, mikä osa on tärkeintä yrityksen toiminnan kannalta.

5.1 Laitteistojen suojaaminen

Kaikki elektroniikka on alttiina erilaisille tietoturvauhille, kuten luonnollisille ja työntekijöiden tai muiden henkilöiden aiheuttamille ongelmille. Komponenttien tai laitteistojen rikkoontuessa voi työnteon jatkaminen olla mahdotonta ja uuden osan tai laitteen vaihtaminen vanhan tilalle voi kestää kauan. Näihin kaikkiin kuitenkin pystytään varautumaan erilaisin keinoin. Markkinoilla on useita erilaisia järjestelmiä, joiden avulla pystytään turvaamaan yrityksen laitteisto, ohjelmistot tai tiedot.

Vaikka ylimääräisten laitteistojen hankita tuo lisäkuluja yritykselle, ne kuitenkin maksavat pidemmällä aikavälillä itsensä takaisin säästyneiden komponenttien, laitteistojen ja työtuntien myötä.

Luonnolliset uhat

Luonnollisina uhkina voidaan mainita muun muassa tulipalot, sähkökatkokset ja ukonilmat. Näiden aiheuttamat vahingot pystytään torjumaan erilaisilla laitteilla, joiden avulla pystytään suojaamaan yrityksen järjestelmät. Alla käydään läpi yleisimmät välineet, joilla voidaan torjua luonnollisten tuhojen aiheuttamia vahinkoja.

UPS (**U**ninterruptible **P**ower **S**upply)

UPS takaa nimensä mukaisesti jatkuvan virransyötön. Se myös tasoittaa virtapiikit sähköverkosta, joka lisää laitteistojen käyttöikää. Sähkökatkoksen sattuessa se pystyy akkunsa avulla pitämään laitteistot käynnissä muutaman minuutin. Tällä tavoin saadaan aikaa tallentaa työt ja valmistautua koneen sammumiseen. UPS:ia hankittaessa täytyy ottaa huomioon, onko laite yhteensopiva haluttuun käyttöön, onko UPS:n koko ja paikka sopivia, jotta laitetta pystytään tarvittaessa huoltamaan helposti. Suurin UPS:n ongelmista on riittämätön akun kesto. Tästä syystä onkin tärkeää tarkistaa UPS:ää hankittaessa, onko sen akku tarpeeksi suuri pitääkseen kaikki halutut laitteistot tarpeeksi pitkään päällä. (EmersonNetworkPower. s 3)

UPS:n hankintaa täytyy suunnitella tarkkaan, että saadaan täysin yrityksen vaatimuksia täyttävät laitteistot. UPS pystyy jakamaan vain tietyn verran virtaa, joten jos siihen liitetään liian monta laitetta, niin UPS ei pysty pitämään laitteita päällä sähkökatkoksen sattuessa. Tarvittaessa UPS-laitteita voi hankkia useampia. Palvelimille ja työasemille on yleensä omat UPS laitteensa niiden erilaisen virran käytön vuoksi. (David Howell 2012.)

UPS-laitteet on jaettu eri kategorioihin Line-Interaktiivi UPS:t ja On-Line UPS:t. Line-Interaktiivi UPS on sopiva toimisto-olosuhteisiin, kun taas On-Line UPS:t ovat sopivia vaihtoehtoja teollisuusympäristöihin, joissa on suuria jännitepiikkejä tai vaatimuksena on yli 3 kVA:n UPS-laite. (UTU.)

Yrityksen laitteistojen virran kulutuksen mittaaminen olisi hyvä tarkastaa virtamittarilla, jotta saadaan tietää minkälainen UPS-laite tarvitaan. Tyypillinen pöytätietokone käyttää noin 80-250 wattia rasituksesta ja osista riippuen. (Griffith university.)

UPS-laitteen olisi hyvä olla mitoitettu siten, että sen kapasiteetti on 60% volttiamppeeria suurempi, kuin mitä kytkettyjen laitteiden käyttö vaatii. Tällöin saadaan sen verran varakäyntiaikaa, että työt ehditään tallentamaan ja laitteistot saadaan sammutettua turvallisesti. Jos on tarvetta pitempiaikaiselle varakäyntiajalle, niin olisi

suositeltavaa ottaa suurempi UPS-laite. Mikäli UPS-laitteistoa käytetään palvelimessa, niin on suositeltavaa tarkistaa ennen UPS-laitteen hankintaa, että siinä on toiminto, joka lähettää signaalin akun vähetessä palvelimelle. Palvelimeen tulee tällöin asentaa ajurit ja ohjelmistot, jotta palvelin ymmärtää UPS-laitteen lähettämän signaalin. Tällöin palvelin ymmärtää ajaa itsensä alas automaattisesti.

Ylijännitesuojat

Ylijännitesuojat ovat toimivia vaihtoehtoja suojaamaan laitteistoja jännitepiikeiltä. Ne pystyvät suojaamaan kytkettyjä laitteistoja myös ukkoselta. Joissakin ylijännitesuojissa on myös RJ-45-suoja, joka suojaa verkkopiuhan kautta tulevat jännitepiikit. Ylijännitesuojat tulee kuitenkin tarkistaa silloin tällöin, että ne pystyvät suojaamaan laitteistot. Joissakin malleissa on oma indikaattori mukana, joka kertoo onko ylijännitesuoja vielä käyttökelpoinen. Kun salama on kerran iskenyt ylijännitesuojaan, se ei pysty takaamaan 100% suojaa laitteistolle.

Palo ja dataturvakaapit

Jos yrityksessä säilötään arvotavaraa, niin erilaiset turvakaapit ovat hyvä ratkaisu. Tulipalon sattuessa turvakaapit pystyvät pitämään sisällön turvassa 60–90 minuutin ajan. (Düperthal.)

Yksikään yllämainituista suojauskeinoista ei ole välttämätön tietoturvan kannalta, mutta ne tuovat erinomaisen suojan yrityksen resursseille, jos sille nähdään tarvetta.

Inhimilliset vahingot

Kauppa- ja teollisuusministeriön (2006) julkaiseman tietoturvakyselyn mukaan 59 % PK-yrityksistä pitää työntekijöiden tietämättömyyttä ja huolimattomuutta merkittävänä tietoturvauhkana. Lähes jokainen yrityksistä piti käyttäjien tietotasoa jonkin verran tai merkittävästi tietoturvatasoa heikentävänä.

Vahingossa tehtyihin virheisiin sekä tahallisesti aiheutettuihin vahinkoihin tulisi vaikuttaa ennaltaehkäisevästi ja alla käydään läpi tapoja, joilla pystytään estämään kyseisiä uhkia.

Laitteistojen lukitseminen

Laitteistojen lukitseminen niille tarkoitettuun huoneeseen, johon vain luotetuilla henkilöillä on avain voi olla hyvä ratkaisu, jos yrityksen tiloissa liikkuu paljon ulkopuolisia. Jos työasemat ovat kuitenkin yleisissä tiloissa kaikkien käsillä, kuten esimerkiksi kirjastoissa tai tietokoneita jälleenmyyvissä liikkeissä, voi silloin käyttää muunlaisia ratkaisuja, kuten koneiden lukittamista erilaisilla lukoilla. Erityisesti kannettavat tietokoneet kannattaa lukita vaijerilukoilla. Koneiden käyttöä myös voidaan rajoittaa ajoittamalla käyttöjärjestelmän lukittautuminen työaikojen ulkopuolelle.

Käyttöoikeudet

Jos käyttöoikeudet eivät ole kunnossa, niin käyttäjät pystyvät aiheuttamaan ohjelmistoille, käyttöjärjestelmälle tai tiedoille vahinkoa. Tästä syystä tulee tarkkaan määritellä, mihin tietoihin kullakin käyttäjällä on oikeus päästä käsiksi.

Käyttäjät voidaan jakaa erilaisiin käyttäjäryhmiin, kuten esimerkiksi verkossa toimivassa vaateliikkeessä voisi olla myyjät, myyntipäällikkö ja ylläpito. Tässä tapauksessa myyjillä ei ole tarvetta pystyä asentamaan tai poistamaan ohjelmia. Myyjien kuitenkin pitää pystyä tekemään tilauksia, tarkastella annettuja tehtäviä ja asettaa tuotteita myyntiin. Myyntipäälliköllä voisi olla hieman laajemmat oikeudet, kuten esimerkiksi mahdollisuus pystyä tarkastelemaan kaikkia olemassa olevia tilauksia. Ylläpitäjillä tulisi olla kaikki mahdolliset oikeudet. Käyttöoikeudet on määriteltävä tarkkaan, jotta kaikki työssä vaadittu saadaan tehtyä, mutta käyttäjälle ei kuitenkaan anneta oikeuksia muuhun käyttöön.

On tärkeää myös ottaa huomioon, että käytetäänkö yrityksessä paikallisia vai verkkopohjaisia käyttöoikeuksia. Paikalliset käyttäjän oikeudet toimivat vain yhdessä

työasemassa, kun verkkopohjaiset käyttäjän oikeudet toimivat jokaisessa verkkoon liitetyssä työasemassa.

Joskus työntekijöillä voi olla tarvetta saada täysi kontrolli käyttöjärjestelmästä, joten silloin oikea vaihtoehto on antaa kyseiselle käyttäjälle paikalliset pääkäyttäjän oikeudet. Niiden tulisi olla erillisen tunnuksen takana, sillä niillä voidaan saada paljon vahinkoa aikaan huolimattoman käytön seurauksena tai hyökkäyksen tullessa.

Jos työntekijällä on tarve päästä ainoastaan omaan työasemaansa käsiksi kaikilla oikeuksilla, niin verkkopohjaisille pääkäyttäjän oikeuksille ei ole tarvetta. Pääkäyttäjän oikeuksia ei kuitenkaan suositella annettavan muille, kuin ylläpitäjille.

5.2 Ohjelmistojen suojaaminen

Tietokoneen ollessa yhdistettynä internettiin, on mahdollisuus saada haittaohjelmia koneelle tai joutua hyökkäyksen kohteeksi. Ohjelmistojen suojaus on yksi tärkeimmistä asioista mietittäessä tietoturvaa. Ohjelmat, käyttöjärjestelmät ja tietokantaohjelmat on kuitenkin mahdollista suojata suhteellisen helposti. Alla käydään läpi erilaisia ohjelmia, jotka suojaavat tietokoneen sisällön.

Viruksentorjuntaohjelmisto

Viruksentorjuntaohjelmistot suojaavat järjestelmää haittaohjelmilta. Viruksien lisäksi ne suojaavat yleensä myös troijalaisilta, madoilta ja rootkiteiltä.
Viruksentorjuntaohjelmistoja löytyy monia erilaisia, mutta yksikään ei pysty tarjoamaan 100 % suojaa, sillä uusia haittaohjelmia tulee jatkuvasti lisää. Ajantasalla oleva viruksentorjuntaohjelmisto antaa kuitenkin melko hyvän suojan.

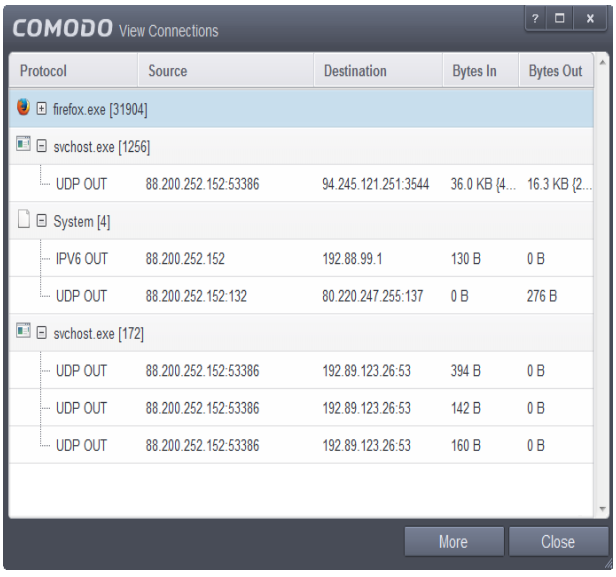
Virustorjunnoissa olevan tarkan manuaalisen skannerin lisäksi niissä on yleensä myös reaaliaikainen skanneri, mikä tutkii päällä olevia prosesseja ja käytettäviä tiedostoja. Osassa virustorjuntaohjelmistoista on jonkin sortin palautustyökalu, jolla saadaan palautettua tiedostot alkuperäiseen tilaan, jos ne joutuvat haittaohjelman saastuttamaksi.

Osa virustorjuntaohjelmistoista käyttää heuristista analyysiä viruksien etsimisessä. Heuristisen analyysin tarkoitus on etsiä uusia ja tuntemattomia haittaohjelmia. Esimerkiksi virus voi muuttaa itseään siten, että viruksentorjuntaohjelma ei pysty tunnistamaan sitä. Tätä varten on tehty heuristinen analyysi, joka ikään kuin arvaa onko tiedosto haittaohjelma vai ei. Heuristinen analyysi on nopea tunnistamaan keskenään samankaltaiset haittaohjelmat. Huonona puolena on se, että virustorjuntaohjelmisto voi antaa vääriä hälytyksiä tiedostoista, jotka eivät ole haittaohjelmia.

Mikään virustorjuntaohjelmisto ei kuitenkaan suojaa verkkoliikenteen kautta tulevilta hyökkäyksiltä, vaan verkkoliikenteen hallitsemiseen tarvitaan erikseen palomuuri.

Palomuurit

Palomuurit ovat järjestelmiä, joiden avulla pystytään kontrolloimaan sisään tai ulospäin kulkevaa verkkoliikennettä. Ne ovat erinomaisia apuvälineitä erilaisia hyökkäyksiä vastaan, sillä ne toimivat ennalta ehkäisevänä turvana, kun taas virustorjunta suojaa vasta silloin, kun ongelma on jo koneella.



Kuvio 1. Comodo Firewall mahdollistaa aktiivisten yhteyksien käytön tarkkailun.

Nykyisissä palomuureissa on mahdollista tarkastella tilastoja verkon käytöstä kuvion 1 mukaisesti, joka auttaa käyttäjää näkemään esimerkiksi, että minne milläkin koneella on aktiivisia yhteyksiä. Palomuuri onkin yksi tärkeimmistä tietoturvan osista, sillä se pystyy estämään ei-toivottuja yhteyksiä. Palomuuri ei kuitenkaan suojaa suoranaisesti viruksilta tai haittaohjelmilta, jos käyttäjä lataa niitä itse tietokoneelle.

Laitepalomuurit

Laitepalomuuri on erillinen laite, jonka päätoiminen tehtävä on verkon liikenteen suodattaminen ja tunnetuimpien haittojen pääsyn estäminen yrityksen verkkoon. Laitepalomuuri siis suojaa koko verkkoa, kun taas ohjelmallinen palomuurit ovat työasemakohtaisia. Laitepalomuuri ei kuitenkaan tee työasemien omista palomuureista hyödyttömiä, vaan se vahvistaa tietoturvan tasoa huomattavasti.

Laitepalomuureilla on omat vahvuutensa, minkä vuoksi niitä kannattaa käyttää. Ne voivat olla tehokkaita jo pienellä konfiguroinnilla ja ne suojaavat jokaisen verkon laitteen. Ne ovat aina päällä ja toimivat vaikka tietokoneessa olisi ongelmia. Haittaohjelmat eivät pysty sammuttamaan laitepalomuuria komennoilla.

On erittäin suositeltavaa, että yritykseen hankittaisiin laitepalomuuri tietoturvan maksimoimiseksi. Laitepalomuuri ja ohjelmallinen palomuuri yhdessä tuovat hyvän suojan yritykselle erilaisia hyökkäyksiä vastaan.

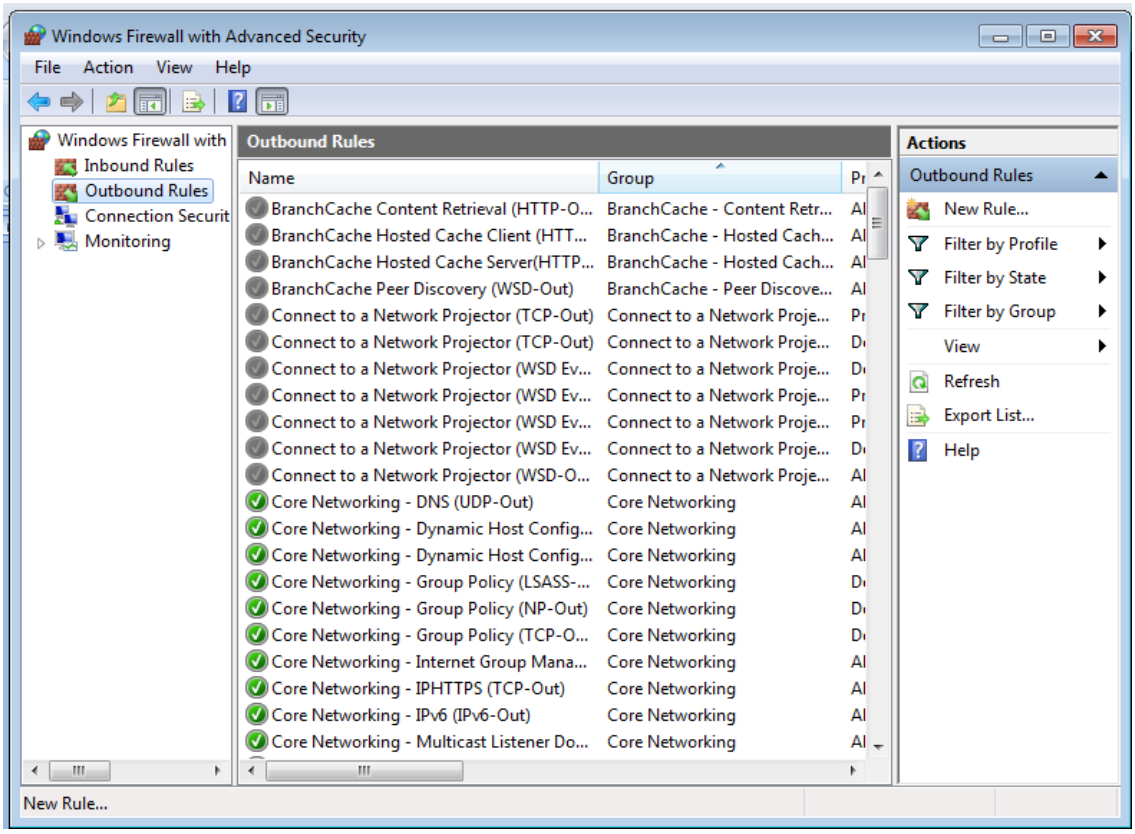
Ohjelmalliset palomuurit

Ylivoimaisesti suosituin palomuuri kotikäyttäjillä on ohjelmallinen palomuuri. Ne antavat käyttäjälle mahdollisuuden kontrolloida ohjelmien verkon käyttöä ja suojaavat yleisimmiltä uhilta. Ohjelmalliset palomuurit suojaavat vain niitä laitteita, mihin ne ovat asennettuina. Hyvä palomuuri ei vie paljoa tietokoneen resursseja ja toimii taustalla siten, ettei se häiritse tietokoneen käyttöä.

Windowsin palomuuri

Windows -käyttöjärjestelmissä on myös oma palomuuri, mikä toimii, kuten muutkin palomuuriohjelmat. Oletusasetuksilla se estää vain ei-halutut sisään tulevat yhteydet. Windowsin oma palomuuri voi olla ihan riittävä ratkaisu, koska oikeanlaisilla asetuksilla se suojaa järjestelmän ihan yhtä hyvin, kuin muutkin palomuurit. Tosin sen käyttö on hankalampaa, sillä muihin palomuureihin verrattuna Windowsin palomuurin käyttöliittymä on melko vaikeaselkoinen, kuten kuvio 2:sta selviää. Sen avulla ei

myöskään pystytä tarkastelemaan, kuinka paljon mikäkin ohjelma käyttää verkkoa. Osaavissa käsissä siitä saa kuitenkin erinomaisen suojan. (Chris Hoffman 2013.)



Kuvio 2. Windows palomuurille pystyy asettamaan tarkat säännöt eri yhteyksille.

Kolmannen osapuolen ohjelmalliset palomuurit

Windowsin oman palomuurin lisäksi on myös useita muitakin vaihtoehtoja, jos kaipaa palomuuriltaan monipuolisempia asetuksia, kuten käyttäjäystävällisemmän käyttöliittymän ja mahdollisuuden tarkastella ohjelmien yhteyksien käyttöä. Jotkut palomuureista myös tallentavat logeja sekä antavat yksityiskohtaisempaa tietoa palomuurin toiminnasta. Useimmille käyttäjille kolmannen osapuolen palomuurit hankaloittavat käyttöä monimutkaisuutensa vuoksi.
(Chris Hoffman 2013.)

Jos yritys ei koe Windowsin omaa palomuuria riittäväksi, yrityksellä ei ole mahdollisuutta tai halua maksaa tietoturvasta, niin voidaan pohtia kolmansien osapuolien tarjoamia ilmaisia palomuureja. Ne yleensä sisältävät suppeamman määrän

ominaisuuksia, mutta pystyvät kuitenkin tarjoamaan riittävän tehokkaan suojan erilaisilta hyökkäyksiltä.

Tilalliset ja tilattomat palomuurit

Palomuurit voivat olla kahta eri tyyppiä: tilallisia ja tilattomia. Nämä sopivat eri käyttötarkoituksiin, ja niillä on omat vahvuutensa ja heikkoutensa. Tilallinen palomuuri antaa enemmän mahdollisuuksia hallita, minkälaisia paketteja palomuurin läpi päästetään. Tilalliset palomuurit pystyvät kertomaan yhteydestä erilaisia tietoja, kuten onko yhteys auki, lähetetty, synkronoitu, synkronointi todennettu tai hyväksytty. Se myös pystyy kertomaan yhteyden muuttumisesta ja pakettien pirstaloitumisesta.

Tilaton palomuuri tarkistaa yhteyden lähteen, sen määränpään ja muita staattisia arvoja. Näistä arvoista tarkistetaan, että päästetäänkö yhteys läpi. Tilaton palomuuri käyttää yksinkertaisia määrityksiä ja se ei esimerkiksi tarkista, että onko yhteyden sisältöä muutettu mitenkään. Tämä helpottaa palomuurin murtamista ja haitalliset yhteydet pääsevät helpommin lävitse. Tilaton palomuuri on kuitenkin nopeampi käsittelemään suuria yhteysmääriä.

Tilallinen palomuuri on hyvä työasemaan paremman turvallisuutensa vuoksi, kun taas tilaton palomuuri on parempi vaihtoehto palvelimille nopeutensa vuoksi.

Hunajapurkit

Toisin kuin viruksentorjunta ja palomuuriohjelmistot, hunajapurkki ei varsinaisesti suojaa järjestelmää vaan ne torjuvat tietyn niille asetetun ongelman. Ne pystyvät tunnistamaan hyökkäyksiä monipuolisesti, kuten esimerkiksi kryptattuja verkkohyökkäyksiä ja internetin luottokorttihuijauksia. Hunajapurkkien monipuolisuus on se syy, minkä vuoksi ne ovat niin tehokkaita.

Kuten aiemmin mainittiin, hunajapurkit eivät suoranaisesti suojaa järjestelmää mutta ne houkuttelevat hyökkääjää käyttämään hunajapurkkia niiden alkuperäisen kohteen sijaan. Niiden vahvuutena voidaan mainita niiden mahdollisuus toimia erilaisissa rooleissa ja

niiden erilaisuuden vuoksi hyökkääjä ei välttämättä tiedä, että onko kyseessä hunajapurkki vai ei.

Hunajapurkki voi estää hyökkäykset useilla eri tavoilla, kuten tuhlaamalla hyökkääjän aikaa. Hyökkääjä voi tässä tilanteessa antaa periksi ja lopettaa hyökkäyksen. Jos hyökkääjällä ei ole varmuutta minkälaisessa roolissa ja miten hunajapurkki toimii yrityksessä, niin hyökkäys voi jäädä tekemättä.

Hunajapurkit ovat luotuja keräämään tietoa ja ne tallentavat kaiken vuorovaikutuksen, mitä niiden kanssa tehdään. Hunajapurkkien avulla pystytään oppimaan ja saamaan arvokasta tietoa hyökkäyksestä, jolloin pystytään suojautumaan paremmin vastaavankaltaisia hyökkäyksiä vastaan tulevaisuudessa.

Hunajapurkin resurssivaatimukset ovat hyvin vähäiset, joten on mahdollista käyttää vanhoja ylimääräisiksi jääneitä koneita erilaisiin hunajapurkkitehtäviin. Hunajapurkin yksinkertaisuuden vuoksi sen riittävään toimintaan kelpaa jopa 128 megatavun muistilla varustettu tietokone ja sillä pystytään hoitamaan vaikka verkon emulointitehtäviä. (Lance Spitzner 2003.)

5.3 Tietojen suojaaminen

Arkaluontoista tietoa käsiteltäessä on tärkeää ottaa huomioon erilaiset tietoja uhkaavat tekijät. Tiedon suojaamiseen on kuitenkin kehitetty erilaisia menetelmiä, joilla saadaan estettyä tahattomat virheet ja tahallisesti aiheutetut haitat.

Varmuuskopiointi

Varmuuskopioinnin ensisijaisena tarkoituksena on palauttaa tiedostot, jotka ovat tavalla tai toisella poistettuja tai korruptoituneita. Esimerkiksi kiintolevyjen rikkoutuminen voi aiheuttaa tietojen katoamista. Tiedostojen varmuuskopioimiseen voidaan käyttää erilaisia tiedonsiirtovälineitä, kuten muistitikkuja, cd- ja dvd-levyjä, nauha-asemia, toisia kiintolevyjä tai palvelinta.

Tietoja kopioitaessa cd-levyille ja muistitikuille on hyvä ottaa huomioon myös niiden riskit, kuten esimerkiksi muistitikut ja cd- sekä dvd-levyt voivat kadota tai rikkoontua helposti. Niiden lyhyen käyttöiän vuoksi niitä joutuu myös kopioimaan muille tallennusmedioille, etteivät tiedot huku. Cd- ja dvd-levyt kuluvat ajan myötä, joten niihin kannattaa suhtautua varauksella.

Palvelimelle kopioitaessa on kuitenkin hyvä ottaa kopio palvelimen varmuuskopioista, sillä kiintolevyt kuluvat ja hajoavat ajan myötä. Kolmessa vuodessa kiintolevyjen hajoamistahti nousee 11.8 %, joten viimeistään silloin olisi hyvä pohtia uusien kiintolevyjen hankkimista. (Juha Tuppi, 2013.)

Nauha-asemat ovat myös yksi vaihtoehto, mutta korkean hintansa vuoksi ne eivät välttämättä ole paras valinta. Nauha-asemat ovat kuitenkin ainoa luotettava vaihtoehto, kun on kyseessä suuret datamäärät, joita tarvitsee säilyttää pitempiä aikoja. Kuitenkin tavalliset kiintolevyt riittävät useimmiten varmuuskopiointiin riittävän hyvin.

Tiedostoja voidaan myös siirtää verkkoon erilaisiin luotettaviin pilvipalveluihin, jos on varmennettu palvelun tarjoajan luotettavuus. Jos yrityksessä on palvelin, olisi hyvä saada kaikki tieto työasemilta kopioitua kyseisen palvelimen kiintolevyille.

On myös hyvä ottaa huomioon, että kaikkea arkaluontoista ei välttämättä kannata laittaa kolmansille osapuolille. Koskaan ei voida olla varmoja siitä, että kuka tiedostot loppujen lopuksi näkee. Arkaluontoista tietoa ei mielellään siirretä ollenkaan kolmansille osapuolille.

Jotkut ohjelmat sisältävät automaattisen varmuuskopiointitoiminnon, joka tallentaa tiedot ennalta määritettyinä väliaikoina haluttuun sijaintiin. Tällaiset toiminnot olisi hyvä ottaa käyttöön, sillä ne estävät työn hukkumisen inhimillisen virheen, sähkökatkon tai muun syyn johdosta.

Varmuuskopiointeja on erityyppisiä, joiden oikea oppisella käyttämisellä pystytään saamaan kaikki hyöty irti varmuuskopioimisesta. Eri varmuuskopiointitavat ovat **inkrementaalinen**, **differentiaalinen** ja **täysi**. (Types of Backup.)

Inkrementaalisessa varmuuskopioinnissa kopioidaan vain ne tiedostot, jotka ovat muuttuneet **viimeisimmän varmuuskopioinnin** jälkeen. Se on nopea tehdä ja se vie vähiten tilaa, eikä se luo ylimääräisiä duplikaattitiedostoja. Tiedostojen palauttaminen on kuitenkin hidasta ja se tarvitsee kaikki varmuuskopiointitiedostot pystyäkseen palauttamaan aiemmat tiedostot. (Types of Backup.)

Differentiaalisessa varmuuskopioinnissa tehdään varmuuskopiot niistä tiedostoista, jotka ovat muuttuneet **viimeisimmän täydellisen varmuuskopioinnin** jälkeen, eli kun on tehty **täysi** varmuuskopiointi, niin kaikki sen jälkeen muuttuvat tiedostot varmuuskopioidaan. Tiedostot ovat nopeampia palauttaa, kuin inkrementaalisen varmuuskopioinnin tiedostot ja tällä tavoin ei tarvita muuta kuin täysi varmuuskopio ja viimeisin differentiaalinen varmuuskopio tiedostojen palautukseen. Varmuuskopioinnin tekeminen on hitaampaa differentiaalisella, kuin inkrementaalisella tavalla ja se luo paljon duplikaattitiedostoja. (Types of Backup.)

Täydessä varmuuskopioinnissa tehdään kopio kaikista tiedostoista. Tällä tavoin tehty varmuuskopiointi on hitainta ja se vie eniten tilaa. Palauttaminen on kuitenkin kaikkein nopeinta ja se tarvitsee vain viimeisen täyden varmuuskopioinnin palauttamista varten. Täysi varmuuskopio vaatii myös eniten tilaa ja tekee paljon duplikaattitiedostoja. (Types of Backup.)

Näitä yhdistelemällä saadaan tehokas varmuuskopiointijärjestelmä, jonka avulla pystytään saamaan kaikki tiedostot talteen ja helposti palautettavaksi tarvittaessa. Olisi hyvä suunnitella yrityksen tarpeet täyttävä varmuuskopiointisuunnitelma, joka takaa sen, etteivät työt koskaan mene hukkaan.

Yleensä täysi varmuuskopiointi otetaan kerran viikossa. Sitten on yrityksen oma päätös, että käytetäänkö inkrementaalista tai differentiaalista varmuuskopiointia. Differentiaalisessa kopioidaan muuttuvat tiedostot ja sitä suositellaan käytettäväksi kerran päivässä. Inkrementaalisella varmuuskopioinnilla pystytään tekemään varmuuskopiot halutessa tunnin välein tai jopa useammin. Tällä tavoin toimimalla pystytään palauttamaan mikä tahansa tiedosto tai tilanne viikon ajalta. (Acronis.)

Inkrementaalinen varmuuskopiointi on paljon joustavampi kopioinnin tekemisen suhteen. Tiedostojen palauttaminen on kuitenkin paljon hitaampaa, koska kaikki tiedostot palautetaan alkuperäisestä täydestä varmuuskopioinnista ja kaikki sen jälkeiset muutokset inkrementaalisista varmuuskopioista. (Acronis.)

Tärkeää on myös testata, että varmuuskopiointi on toiminut. Olisi hyvä tarkistaa varmuuskopioinnin toimivuus, sillä joissakin tilanteissa virheellisten asetusten tai muiden syiden vuoksi varmuuskopiointi ei toimi oikein ja se voi aiheuttaa arvokkaiden tietojen menetyksen.

Tiedon kryptaus

Tiedon salaaminen, eli kryptaus on erinomainen keino estää ulkopuolisia pääsemästä käsiksi arkaluontoisiin tiedostoihin. Kryptaus tapahtuu siten, että käytetään ohjelmaa, jolla kryptataan tiedosto erilaisilla algoritmeilla. Kryptaaminen ei varsinaisesti suojaa tiedostoja, mutta se estää ulkopuolisilta niiden lukumahdollisuuden. Vaikka ulkopuolinen henkilö saisikin kryptatun tiedoston käsiinsä, hän ei välttämättä saa sitä koskaan auki.

Siirrettävän tiedon kryptaaminen on suositeltavaa. Liikutettiin sitten tiedostoja verkon välityksellä tai fyysisellä medialla, kuten ulkoisilla kiintolevyillä tai USB-tikuilla, niin salattuja tietoja ei saada auki vaikka siirtomedia häviää tai varastetaan.

Langattoman verkon suojaaminen

Langattomien verkkojen suojaaminen on tärkeää, sillä ulkopuoliset pystyvät muuten tarkastelemaan verkon sisältöä. Langattoman verkon liikenteen salaus onnistuu WEP, WPA ja WPA2 salausmenetelmillä. (webopedia 2007.)

WEP oli oletuksena langattoman verkon suojausmenetelmänä ensimmäisissä langatonta verkkoa käyttävissä laitteissa mutta nykyisemmin WEPin käyttö on vähentynyt sen helpon murrettavuuden takia. (webopedia 2007.)

WPA salausmenetelmä on WEP:n jälkeen kehitetty salausmentelmä, jossa on korjattu kaikki WEP:n puutteet. Se käyttää TKIP protokollaa, joka tarkastaa langattomassa verkossa lähetettyjen pakettien eheyttä. (webopedia 2007.)

WPA tähtää vahvempaan tiedon salaukseen, kuin WEP mutta joka laitteen tulee käyttää WPA salausta, tai muuten laitteet vaihtavat salauksen WEPpiin. (webopedia 2007.)

WPA2 on samanlainen, kuin WPA muuten mutta siinä on lisäksi standardin mukainen järjestelmäsalaus AES. WPA2:sta on myös kaksi eri versiota: WPA2 Personal ja WPA2 Enterprise. WPA2 Personal sopii kotikäyttöön ja pienille yrityksille, kun taas WPA2 Enterprise on isommille yrityksille sopiva. Erona on se, että Enterprise version käytössä tarvitaan RADIUS tunnistautumispalvelimen käyttöä.

RADIUS palvelin mahdollistaa keskitetyn käyttäjätunnuksien tunnistamisen ja hallinnoinnin verkonkäyttäjille, sekä antaa paremmin tietoa verkon käytöstä.

Tiedostojen poisto ja palautus

Tiedostojen oikeaoppinen poistaminen on tärkeää, kun hankkiudutaan eroon vanhoista kiintolevyistä. Ulkopuoliset voivat saada käsiinsä vanhat kiintolevyt tavalla tai toisella, joten tietojen joutuminen vääriin käsiin on mahdollista.

Kun tiedosto poistetaan, niin tiedot eivät häviä kiintolevyltä lopullisesti. Sektori, jossa kyseinen tiedosto sijaitsee, merkataan siten, että siihen voi kirjoittaa uutta tietoa päälle. Tiedot katoavat vasta silloin, kun niiden päälle kirjoitetaan uutta tietoa.

Poistettujen tiedostojen ylikirjoittamista varten on tehty erillisiä ohjelmia, jotka hoitavat ylikirjoituksen nopeasti moneen kertaan. Ylikirjoitus olisi hyvä tehdä useammin kuin yhden kerran, jotta kaikki tieto saadaan varmasti hävitettyä lopullisesti.

Tiedostot pystytään myös palauttamaan, jos tiedostojen poistamisesta ei ole kulunut kauaa aikaa. Mitä aiemmin tiedostot yritetään palauttaa, niin sitä suuremmalla todennäköisyydellä onnistutaan, sillä uutta tietoa ei ole välttämättä ehditty kirjoittaa vielä vanhan tiedon päälle.

Joissakin tapauksissa on uskottu, että kovalevyn alustaminen tai osiointi riittää poistamaan tiedostot, mutta ne vain poistavat tiedostoihin käyttöjärjestelmän tekemät viittaukset. Tiedostot pystytään palauttamaan suhteellisen helposti näissä tapauksissa.

Järjestelmän palautus

Käyttöjärjestelmät ja ohjelmistot rikkoontuvat usein, joten niiden nopea palautus on tärkeää, ettei arvokasta työaikaa mene hukkaan. Yksittäinen ohjelma voidaan korjata helposti uudelleen asentamalla, mutta käyttöjärjestelmän ja siihen kaikkien tarvittavien ohjelmien asentaminen vie yrityksen resursseja.

Yrityksen palvelinta pystytään käyttämään nopeaan palauttamiseen, sillä on erilaisia ohjelmia, joiden avulla pystytään palauttamaan kone verkon kautta nopeasti. Jos yrityksellä on monta samanlaista tietokonetta, asennetaan yksi tietokoneista käyttövalmiiksi siten, että käyttöjärjestelmä on päivitetty ja ohjelmistot ovat asennettuina. Tämän jälkeen luodaan palautusohjelmalla tietokoneen kovalevystä image-tiedosto, joka on eräänlainen kopio kaikesta tietokoneen sisällöstä. Tämän kopion avulla pystytään palauttamaan kaikki vastaavanlaiset koneet verkon kautta hetkessä siihen tilaan, mitä image-tiedoston luomiseen käytetty kone oli imagen luontivaiheessa.

Käyttöjärjestelmän ja ohjelmistojen päivittäminen

Käyttöjärjestelmän ja ohjelmistojen pitäminen ajantasalla on erittäin tärkeää, sillä silloin saadaan paikattua erilaiset tietoturva-aukot, jotka ohjelmiston tarjoaja on löytänyt ja korjannut. Päivittämättömät ohjelmistot ja käyttöjärjestelmät voivat saastuneina levittää yrityksen verkkoon haittaohjelmia ja saastuttaa muut yrityksen laitteistot.

Päivitysten lataaminen jokaiselle koneelle on erikseen hidasta ja vie paljon kaistaa internet yhteydeltä, joten tehokkain tapa päivittää yrityksen työasemat on ladata päivitykset yrityksen palvelimelle, josta ne jaetaan sisäverkon kautta kaikille laitteille. Tämä nopeuttaa päivittämistä huomattavasti ja voidaan olla varmoja siitä, että päivittäminen on onnistunut.

Tietoturvan ulkoistaminen

Tietoturvan ulkoistaminen voi olla hyvä vaihtoehto silloin, kun yrityksellä ei ole halua ja/tai taitoa itse hoitaa omaa tietoturvaansa. Yleensä kuitenkin tietoturvapalveluista tietämättömällä yrityksellä ei ole selvää, minkälaisia palveluita tarvitaan. Tällöin voi tulla paljon kustannuksia, eikä rahalle saada vastinetta. (Kari Kemppainen 2005.)

Vaikka yrityksen tietoturva ulkoistettaisiinkin, se ei vapauta yritystä kaikesta vastuusta, vaan kokonaisnäkemys on pidettävä omassa yrityksessä. Jos yrityksen omat resurssit eivät riitä, niin kokonaisuuden valvonnan voi ostaa toisesta yrityksestä. Pitää kuitenkin ottaa huomioon, ettei ulkoisteta liikaa ja luoteta siihen, että asiat ovat sen jälkeen kunnossa. (Kari Kemppainen 2005.)

Jos valvontaa ei suoriteta, eikä yrityksellä ole tietoa tietoturvasta ja tilatuista tietoturvapalveluista, niin ongelmien sattuessa ulkoistava yritys voi kiertää vastuunsa. He voivat vedota siihen, että yrityksessä ei ollut tarkkaan määritelty, minkälaista tietoturvaa yrityksessä haluttiin ja tarvittiin. (Kari Kemppainen 2005.)

5.4 Henkilökunta

Yrityksessä työskentelevien henkilöiden turvaaminen tuo omat haasteensa ja on tehtävä erilaisia menetelmiä, joilla estetään yrityksen resurssien tahaton ja tahallinen väärinkäyttö työntekijöiden päästessään niihin käsiksi. Ulkoisten uhkien yleistyessä on myös otettava huomioon yrityksen sisäisten uhkien mahdollisuus. Yleisimmät riskit ovat:

Puutteelliset toimintatavat

Yrityksessä tulee olla yleiset tietoturvakäytännöt ja ohjeistukset sekä työntekijöitä tulee valvoa ja kouluttaa. Ilman koulutusta ja ohjeistusta työntekijät eivät pysty välttämättä toimimaan tietoturvallisesti. (Valtiovarainministeriö 2003, s. 31-32)

Tahattomat teot

Erilaisiin vahingossa tehtyihin virheisiin on hyvä varautua, kuten ohjelmankäytössä tai tiedonsyötössä tehtyisiin virheisiin. Työntekijät pystyvät myös levittämään viruksia ladatessaan tiedostoja sähköpostista tai siirtäessään tietoa siirrettäviltä medioilta, jotka ovat olleet kotona käytössä. Usein virheitä tapahtuu myös ylläpidon puolella ja huoltotoimenpiteissä, kuten tietojen kadottaminen, väärien asetusten määrittely tai väärin asennetut ohjelmistot. (Valtiovarainministeriö 2003, s. 31-32)

Tahalliset teot

Joskus työntekijät saattavat tuhota, muuttaa tai anastaa yrityksen tietoja tahallisesti eri syistä johtuen. Muita yleisiä tapauksia on tietokantoihin tunkeutuminen, tietoverkon salakuuntelu ja toisten käyttöoikeuksilla toimiminen. Näitä on todella vaikeaa estää tapahtumasta, sillä työntekijöillä on mahdollisuus päästä käsiksi ainakin joihinkin yrityksen tietoihin. (Valtiovarainministeriö 2003, s. 31-32)

Ylivoimainen este

Ylivoimaisiksi esteiksi voidaan laskea avainhenkilöstön menetys, lakko tai muu työntekoa estävä tapahtuma. Näihin on vaikea varautua eikä niihin ole yhtä ainoaa oikeaa ratkaisua, vaan on toimittava tilanteen mukaan.

6 Hyökkäyksien torjuminen

Tyypilliset hyökkääjät pystytään jakamaan erilaisiin ryhmiin. Erilaisia tietoturvaa uhkaavia hyökkääjiä ovat muun muassa

Amatöörit

Amatöörit toimivat mahdollisuuden saadessaan, eli he voivat kirjautua muiden tunnuksilla sisään, jos he löytävät käyttäjätunnuksen ja salasanan. Nykyään mobiililaitteissakin on automaattinen kirjautuminen eri sivustoille, joka helpottaa amatöörihyökkääjien toimintaa.

Amatööreihin kuuluvat myös "script kiddiet", joilla ei itsellään ole taitoa tehdä hyökkäyksiä tai haittaohjelmia. He käyttävät valmiita ohjelmia ja valmiita komentosarjoja, joilla loppujen lopuksi he harvoin saavat mitään aikaiseksi.

Hakkerit

Hakkerit ovat hyökkääjiä, joilla ei yleensä ole haitallisia aikomuksia. He voivat murtautua järjestelmiin ja tutkia järjestelmän sisältöä. Hakkerit haluavat tällä tavoin todistaa, että he pystyvät tekemään niin.

Krakkerit

Toisin kuin hakkereilla, krakkereilla on haitallisia aikeita järjestelmään murtautuessaan. He varastavat tietoa ja murtavat järjestelmän suojauksen.

Erilaiset rikollisryhmät

Kyseiset ryhmät etsivät sopivan yrityksen, joihin he yrittävät murtautua erilaisten hyötyjen kuten rahan vuoksi.

Nettiterroristit

Nettiterroristit hyökkäävät erilaisiin järjestelmiin aatteiden tai poliittisen syiden vuoksi.

Valtion tukemat vakoojat ja "IT-sotilaat"

Useilla suurilla moderneilla valtioilla on armeijoita, jotka ovat niin sanottuja IT-sotilaita. Niiden tehtävänä on vakoilla valtioita tai eri maiden armeijoita ja yrittää kerätä digitaalista tietoa eri keinoin. Esimerkiksi Yhdysvalloissa toimiva turvallisuusvirasto NSA oli jäänyt kiinni Saksan vakoilusta vuoden 2013 loppupuolella. (Daniel Soper 2013.)

Hyökkääjiltä vaaditaan kolme asiaa, mitkä johtavat hyökkäykseen: tapa, mahdollisuus ja syy. Tapaan vaaditaan tieto, taito ja välineet, kun taas mahdollisuudella haetaan sopivaa ajankohtaa tai mahdollisuutta päästä käsiksi järjestelmään eri tavoin. Lopuksi on oltava syy, minkä takia hyökkäys tehdään. Jos yksikin näistä kolmesta syystä saadaan poistettua, niin hyökkäys ei voi onnistua. (Daniel Soper 2013.)

Hyökkäyksen sattuessa on eri tapoja miten toimia, joita käydään läpi seuraavaksi

Estä hyökkäys

Hyökkäykset yleensä tehdään jonkin haavoittuvuuden kautta. Jos hyökkäyksen aikana huomataan hyökkääjien käyttämä haavoittuvuus ja se pystytään tukkimaan, niin hyökkäys voidaan saada estettyä.

Hyökkäystä tulisi ainakin vaikeuttaa huomattavasti, jos sitä ei pystytä tekemään mahdottomaksi. (Daniel Soper 2013.)

Harhauta hyökkääjää

Hyökkääjää varten voidaan tehdä esimerkiksi erillinen hunajapurkkipalvelin, joka on hyökkääjälle houkuttelevampi, kuin alkuperäinen kohde. Tällöin hyökkääjä tuhlaa aikaansa ansaksi asetetun hunajapurkin kanssa. (Daniel Soper 2013.)

Lievennä hyökkäystä

Jos hyökkäystä ei pystytä estämään tai hyökkääjää harhauttamaan, niin voidaan yrittää lieventää hyökkäyksen aiheuttamia tuhoja. Varaudutaan siihen, että hyökkäyksellä päästään eri suojausten lävitse ja otetaan käyttöön erilaisia suojausmekanismeja, joilla estetään suuremman vahingon aiheutuminen. (Daniel Soper 2013.)

Havaitse hyökkäys

Jos hyökkäys pystytään havaitsemaan silloin, kun se on etenemässä, niin se ehkä pystytään estämään. On myös tärkeää huomata hyökkäyksen jälkeen, että hyökkäys on tapahtunut, niin voidaan korjata vahingot. Siitä pystytään myös tutkimaan haavoittuvuuksia ja oppimaan virheistä, kuten miten hyökkääjä on murtanut järjestelmän suojauksen. Tämän tiedon avulla huomataan erilaiset haavoittuvuudet ja ne pystytään korjaamaan, jolloin estetään samanlaiset hyökkäykset tulevaisuudessa. (Daniel Soper 2013.)

Hyökkäyksestä palautuminen

Yritys voi tarvita varmuuskopioita kadonneista tiedoista.Olisi hyvä myös tutkia järjestelmä, että mitään ylimääräistä hyökkääjän jäljiltä ei löydy, kuten haittaohjelmia. Hyökkääjän huomatessa järjestelmien nopea palautuminen ja hyökkäyksen aiheuttamien haittojen jääneen mitättömiksi, hän ei välttämättä hyökkää enää uudelleen. (Daniel Soper 2013.)

7 Henkilökunnan perehdyttäminen

Ylen tekemän tutkimuksen mukaan pohjoissavolaiset yritykset ja työnantajat pitivät työntekijöitään suurimpana tietoturvauhkana. Työntekijöille olisi hyvä saada annettua selkeät ja helposti ymmärrettävät ohjeet, jotta yrityksen tietoturva pysyisi kunnossa.

Tärkeää on työntekijää opastaessa myös selittää miksi kyseiset asiat tulee tehdä, sillä muuten työntekijä ei välttämättä ymmärrä työn tärkeyttä ja jättää sen tekemättä päästäkseen nopeammin muiden tehtävien pariin. Alla käydään läpi asioita, mitä olisi hyvä perehdyttää työntekijälle, että yrityksen tietoturva pysyisi kunnossa.

Aina tauolle lähdettäessä on lukittava tai sammutettava tietokone niin, että konetta ei pysty käyttämään ilman salasanaa.

Työaseman lukitseminen on tärkeää aina, kun itse ei olla työskentelemässä. Ulkopuoliset voivat helposti saada paljon vahinkoa aikaiseksi joko keskeneräiselle työlle tai ohjelmistoille ja käyttöjärjestelmälle.

Työasemaa sammutettaessa tulee ottaa huomioon, että mitään ohjelmia ei ole käynnissä tai päivityksiä asentumassa.

Päivitysten aikana tai ohjelmien ollessa käynnissä ei tule sammuttaa tietokonetta. Jos tietokone käyttää ohjelman tai käyttöjärjestelmän tiedostoja ja se sammutetaan kesken tiedoston kirjoituksen, niin pahimmillaan se voi johtaa ohjelman tai käyttöjärjestelmän toimimattomuuteen tiedostojen korruptoituessa.

Siirrettävät mediat (esim. CD-levyt, USB-tikut ja kovalevyt) on aina pidettävä turvallisessa paikassa, johon ulkopuoliset eivät pääse käsiksi.

Kaikki siirrettävät mediat ovat helppoja kohteita hyökkääjälle, jos ne ovat näkyvällä paikalla. Ne voidaan joko varastaa tai niihin voidaan laittaa haittaohjelmia, jolloin ne päätyvät työasemaan ja sitä kautta yrityksen verkkoon.

Siirrettäville medioille ei saa koskaan pistää arkaluontoista tietoa.

Siirrettävät mediat voivat helposti hävitä tai ne voidaan varastaa, jonka vuoksi niihin ei saa tallentaa arkaluontoista tietoa. Kyseisten tiedontallennusvälineiden hävitessä tai vääriin käsiin voidaan aiheuttaa yritykselle korvaamatonta vahinkoa.

Varmuuskopiointi tulisi tehdä säännöllisesti ja muistaa tallentaa työ välillä, jos tekee pidemmän aikaa töitä.

Aina ei kannata luottaa täysin automaattiseen varmuuskopiointiin, vaan pidemmissä työrupeamissa on tärkeää tallentaa usein. Tällä tavoin säästetään arvokkaita työtunteja, jos syystä tai toisesta ohjelma kaatuu ja automaattinen kopiointi ei olekaan toiminut.

Varmuuskopioita olisi myös hyvä tehdä yrityksen verkkopalvelimelle, jos mahdollista.

Kovalevyt ovat kulutustavaraa ja hajoavat suhteellisen usein. Tästä syystä on tärkeää myös kopioida mielellään useammalle erilliselle kiintolevylle, jos se vain on mahdollista. Yrityksen verkkopalvelimen kiintolevylle varmuuskopiointi on siihen sopiva ratkaisu, sillä niihin pääsee käsiksi tarvittaessa muiltakin työasemilta jos ei aina ole mahdollista työskennellä omalta työasemalta.

Työn suojaaminen ulkopuolisilta, eli tauolle lähdettäessä töitä ei jätetä tietokoneen näytölle kaikkien näkyville. Estetään myös olan yli kurkkiminen salasanojen kirjoittamisen aikana sekä jos käsitellään arkaluontoista tietoa.

Varsinkin arkaluonteista tietoa käsitellessä on tärkeää, ettei vuodeta tietoja ulkopuolisille. Koneen voi lukita nopeasti painamalla näppäimistöstä Windows-painiketta, sekä L-kirjainta yhtaikaa.

Vaikean salasanan käyttäminen, johon tulee isoja ja pieniä kirjaimia, numeroita ja mielellään myös erikoismerkkejä. Salasanaa ei pitäisi kenenkään pystyä arvaamaan. Jos joku saa salasanan urkittua tietoonsa, se täytyy vaihtaa heti. Salasana täytyy säilyttää turvallisessa paikassa, jos sitä ei pysty muistamaan.

Hyökkääjät käyttävät salasanojen murtamiseen murto-ohjelmia, jotka sisältävät erilaisia listoja ja sanakirjoja. Näiden listojen ja sanakirjojen avulla hyökkääjä pystyy käymään läpi todella nopeasti käytetyimmät salasanat ja sanat, jotka esiintyvät sanakirjassa.

Salasanan tulisi olla satunnaisista merkeistä koostuva merkkijono, mikä ei muistuta mitään olemassaolevia sanoja. Listoissa on myös otettu huomioon kirjainten ja numeroiden muutokset (1 = i, 4 = a, 0 = o jne.), sekä takaperin kirjoitetut sanat.

Nimet ja muut helposti käyttäjään liitettävät sanat voivat olla helposti arvattavia. Asiantuntijat suosittelevat 15 merkin pituisia salasanoja, joissa on isoja ja pieniä kirjaimia, numeroita ja erikoismerkkejä.

Työpaikan sähköpostia ei tulisi käyttää muuhun, kun työasioiden hoitamiseen. Sähköpostin kautta ei saa lähettää arkaluontoista tietoa.

Henkilökohtaisen sähköpostin kautta voidaan todennäköisemmin ladata haitallisia tiedostoja, sillä sitä käytetään huolettomammin, kuin työpaikan sähköpostia. Ylipäätänsä ei kannata ladata mitään tiedostoja, joiden toiminnasta ei voida olla varmoja.

Sähköpostia ei saa käyttää arkaluontoisen tiedon lähettämiseen, ellei sähköpostiliikennettä ole salattu. Ulkopuoliset osapuolet pystyvät tarkastelemaan viestien sisältöä, salaamatonta liikennettä.

Paperiset dokumentit tulee hävittää aina silppurilla tai muilla vastaavilla hävityskeinoilla.

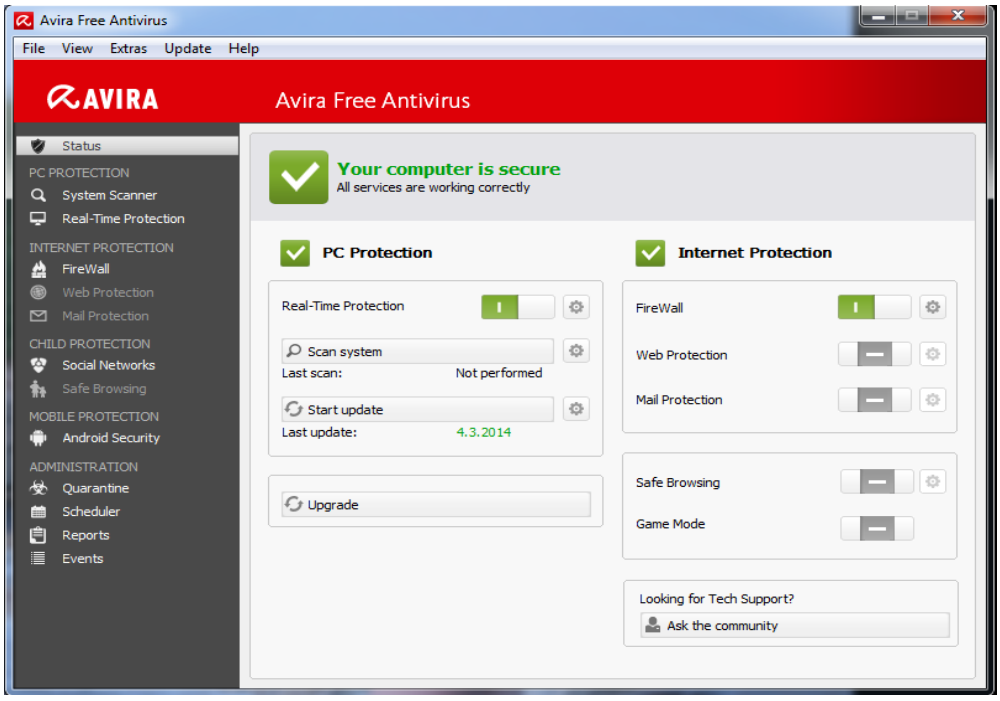
Ulkopuoliset tahot voivat olla kiinnostuneita yrityksen tiedoista ja väärissä käsissä ne voivat aiheuttaa paljon vahinkoa yritykselle, joten paperiset dokumentit tulee hävittää yrityksen omalla silppurilla tai käyttää luotettaa ulkopuolista palvelua, jolloin ammattilaiset hävittävät paperit luottamuksellisesti. Yrityksessä voi myös olla erillinen roskasäiliö hävitettäville dokumenteille.

8 Tietoturvaohjelmistojen käyttöönotto

Tässä osiossa käydään lävitse virustorjunnan ja palomuurin käyttöönotto sekä tyypillisiä asetuksia, mitä on hyvä ottaa huomioon torjuntaohjelmistoja asentaessa.

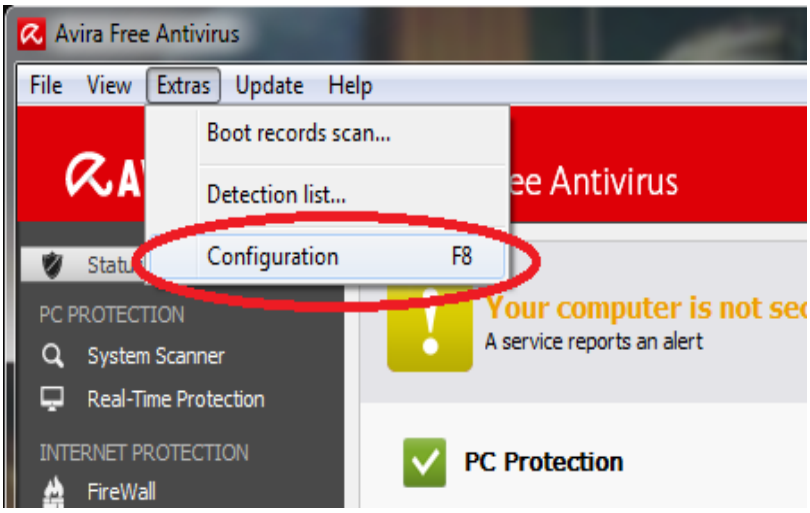
8.1 Virustorjunnan asetukset (Avira Free Antivirus)

Tässä käydään läpi Aviran ilmaista viruksentorjuntaohjelmistoa sen helppokäyttöisyyden ja sen kohtalaisen monipuolisten asetusten vuoksi. Avira Free Antiviruksen ollessa käyttövalmis, sen tulisi näyttää suunnilleen samalta kuin kuvio 3:ssa esitetty tilanne.



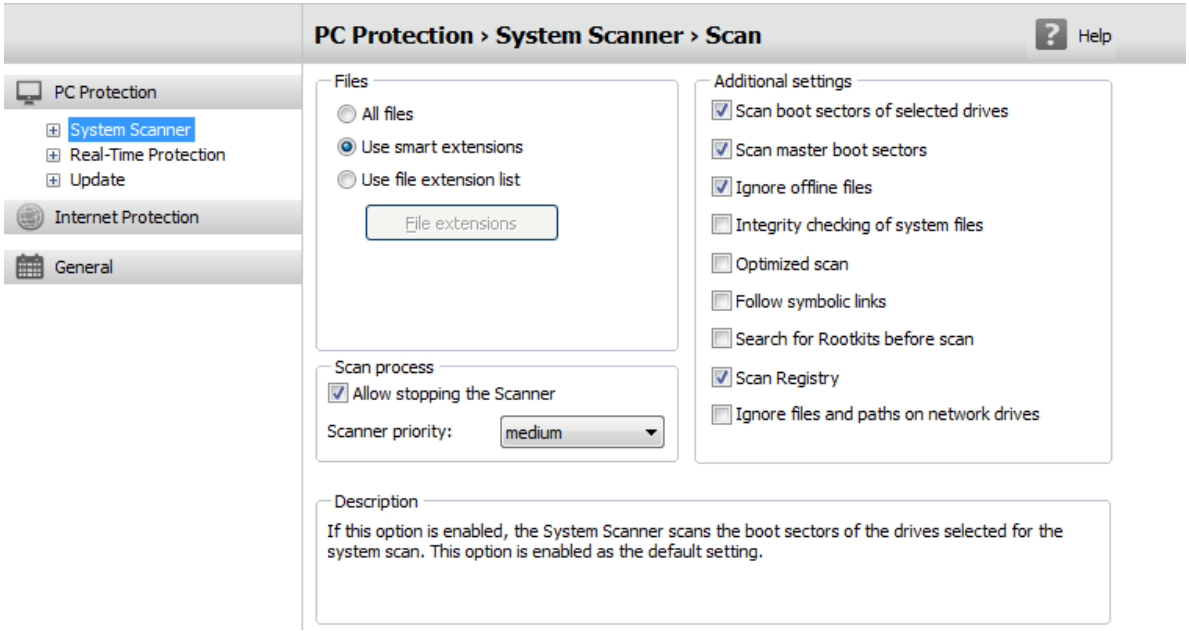
Kuvio 3. Avira Free Antivirus ilmoittaa tietokoneen virustorjunnan ja palomuurin olevan toiminnassa.

Tarkempia asetuksia pääsee valitsemaan Extra alasvetovalikosta painamalla Configuration painiketta kuvio 4:n mukaisella tavalla.



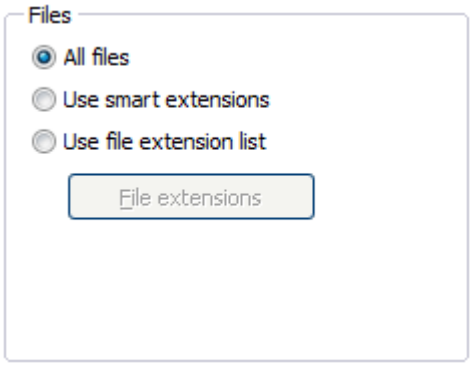
Kuvio 4. Extras alasvetovalikosta päästään muuttamaan Aviran asetuksia.

Tämän jälkeen päästään ikkunaan, josta pystytään määrittelemään virustorjunnan, sekä palomuurin asetuksia. Avirassa ei ole omaa palomuuria, vaan se käyttää Windowsin palomuuria. Virustorjunnan asetukset ovat jaettuna kolmeen osaan: System Scanner, Real-Time Protection, sekä Update, kuten kuvio 5:ssä on esitetty.



Kuvio 5. Aviran virusskannerin oletus asetukset.

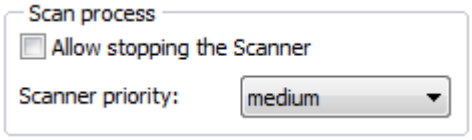
System Scannerissa käydään läpi Antiviruksen skannerin asetukset kuvio 6:n mukaisella tavalla.



Kuvio 6. Virusskannerin asetuksissa on valittu kaikki tiedostot.

Files kohdan alta voidaan päättää, minkälaisia tiedostoja skannataan. Vaihtoehtoja on kolme:
All files - kaikki tietokoneen tiedostot skannataan.
Use smart extensions - ohjelma itse päättää, mitä tiedostoja skannataan tiedostojen tyypin perusteella.
Use file extension list - käyttäjä itse voi määritellä, mitä tiedostoja skannataan.

Kaikki tiedostot olisi hyvä skannnata, etteivät mahdolliset haittaohjelmat jää huomaamatta, joten valitaan **all files**.



Kuvio 7. Skannauksen keskeyttämistä ei sallita.

Scan process kohdassa voidaan valita kuvio 7:n mukaisella tavalla, pystyykö skannauksen keskeyttämään. Tämä on hyvä ottaa pois päältä, ettei käyttäjä pysty pysäyttämään skannausta.

Scanner priority: kohdasta voidaan vaihtaa low, medium tai high. Tällä määritellään se, kuinka paljon koneen resursseja käytetään skannaukseen. Tällä ei ole väliä, jos prosesseja ei ole paljoa, mutta vanhemmilla koneilla voi olla hyvä asettaa prioriteetti lowiksi. Skannauksessa voi kestää kauemmin, mutta se ei haittaa käytettävyyttä. Vastaavasti tehokkaammilla koneilla voidaan asettaa priority high:ksi.

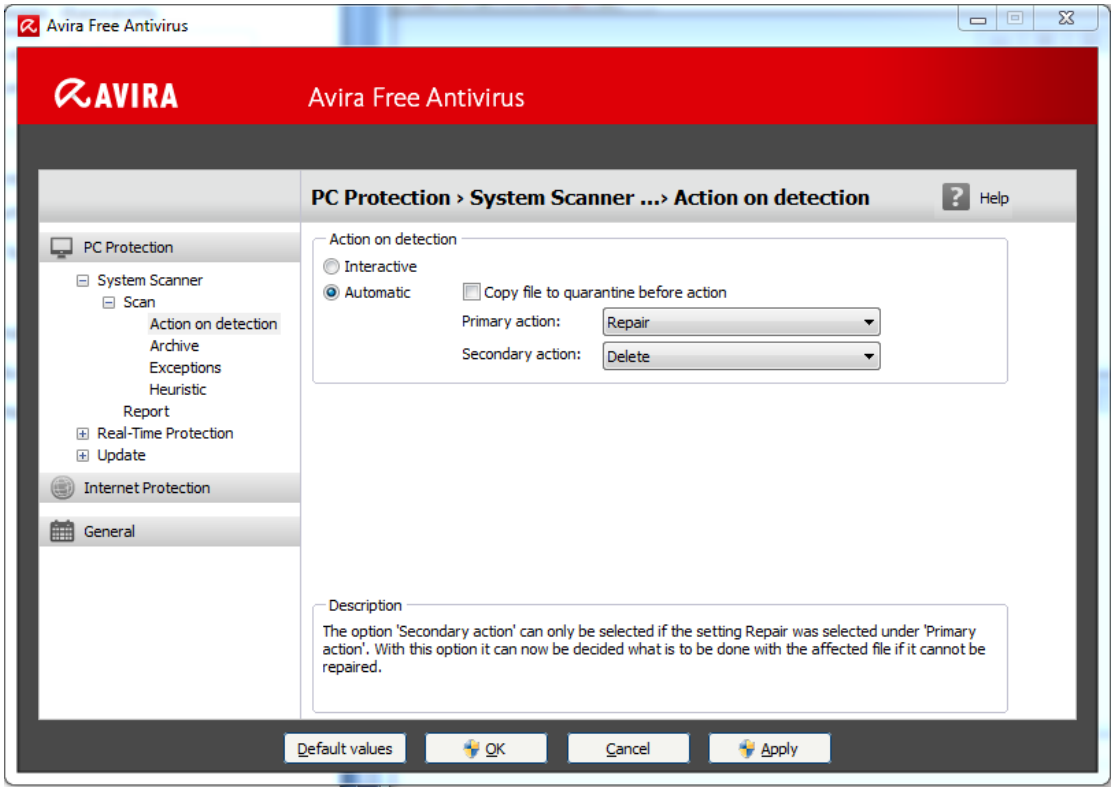
Additional settings kohdasta voidaan määritellä muita asetuksia, kuten esimerkiksi tarkastetaanko poiskytkettyjä tiedostoja tai skannataanko rekisterin tiedostot. Oletuksena nämä tuovat riittävän turvan, joten niihin ei välttämättä tarvitse koskea ollenkaan.

Vasemmassa reunassa PC Protectionin alapuolella oleva **Scan** painike voidaan laajentaa plusmerkistä, jolloin pystytään säätämään skannerin muita asetuksia. Näistä pystytään määrittelemään lisää asetuksia, kuten miten toimitaan skannerin löytäessä haittaohjelmia, mitä arkistoja skannataan, poikkeukset ja heuristisen analyysin havaitsemisherkkyyttä.

Action on detection kohdassa suositellaan valitsemaan automaattiset asetukset. Tällöin ohjelma hoitaa automaattisesti haitalliset tiedostot pois koneelta. Toimintoja on viisi erilaista ja niitä voi asettaa joko ensisijaiseksi ja toissijaiseksi toiminnoiksi. Toiminnot ovat korjaa, nimeä uudelleen, laita karanteeniin, poista ja jätä huomiotta.

Koneen käyttötavasta riippuen on suositeltavaa laittaa ensisijaiseksi toiminnoksi korjaaminen ja toissijaiseksi toiminnoksi poistaminen kuvio 8:n mukaisella tavalla. Tällöin skanneri viruksen löytäessään yrittää korjata sen ja jos se ei onnistu, tiedosto poistetaan.

Kuitenkin tiedoston poistamisen kanssa kannattaa olla varovainen, sillä jos yrityksessä tehdään omia ohjelmia tai käytetään ohjelmia jotka voivat laukaista virushälytyksen. Tällöin heuristisen analyysin pois ottaminen voi olla vaihtoehto, jotta virusskanneri poistaa vain varmaksi tiedetyt virukset. Jos ei luoteta virusskanneriin, eikä haluta poistaa mitään, niin voidaan laittaa toissijaiseksi toiminnoksi haittaohjelman karanteeniin siirtäminen.



Kuvio 8. Skannerin automaattisiksi ensisijaiseksi toiminnoiksi on valittu korjaaminen ja toissijaiseksi poistaminen.

Archive kohdassa määritellään, minkälaisia arkistoja skanneri käy lävitse. Listasta voidaan käydä läpi, minkälaisia arkistoja halutaan tarkastaa ja mitä halutaan jättää väliin. Jos yrityksellä ei ole minkäänlaisia arkistoja, ei tästä kohdasta tarvitse välittää.

Exceptions kohdassa määritellään poikkeukset. Täällä voidaan määritellä, jos jätetään joku tiedosto tai kansio kokonaan skannaamatta.

Heuristic kohdassa pystytään määrittelemään heuristisen analyysin asetuksia. Heuristisen analyysin voi ottaa kokonaan pois päältä tai vaihtaa sen havaitsemistarkkuutta. Oletusasetuksina ne tuovat ihan riittävän turvan, joten niihin ei välttämättä ole tarvetta koskea.

Report kohdassa voidaan päättää, minkälaisia logeja virustorjuntaohjelmisto tekee skannauksesta. Default vaihtoehto on ihan riittävä, sillä se jättää ylimääräiset tiedostot pois ja tallentaa logiin tiedot tartunnan saaneista tiedostoista, jos niitä löydetään.

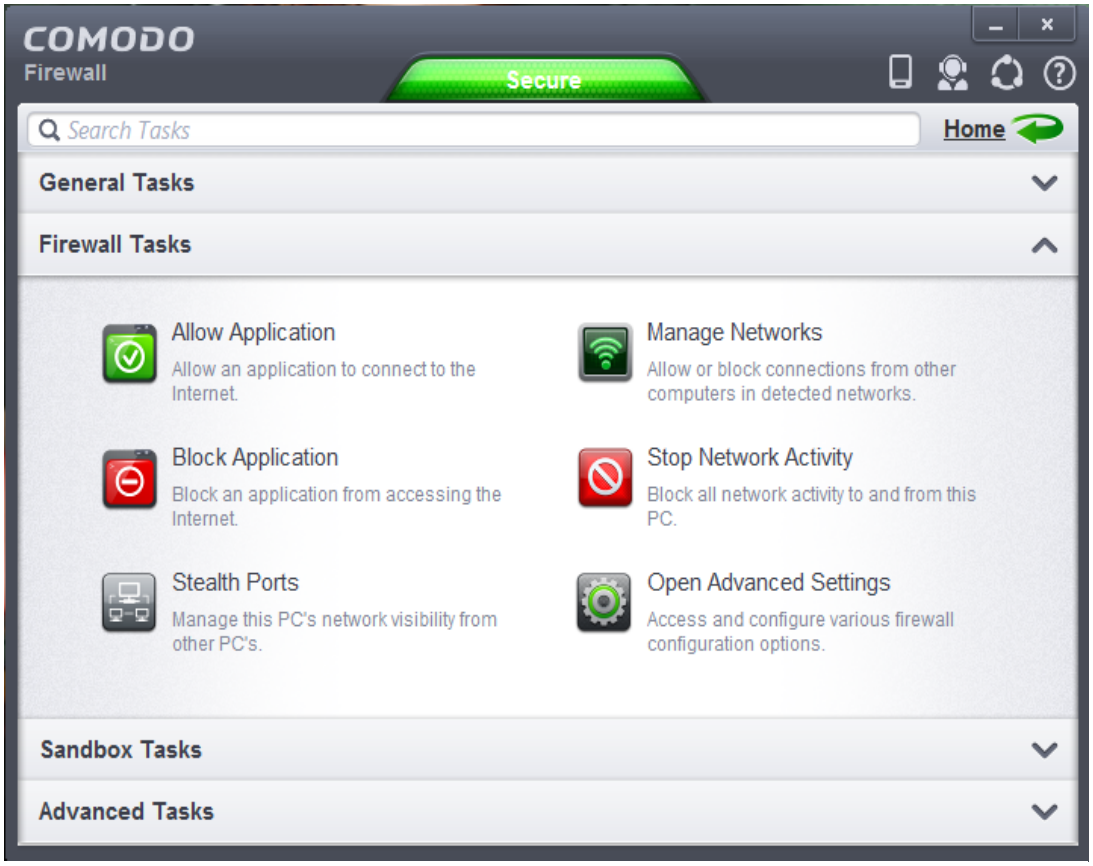
Real-Time Protectionin alta löytyy kaikki samat asetukset, kuin **System Scanner**istakin, mutta ne koskevat vain reaaliaikaisesti toimivaa skanneria. Samat asetukset ovat ihan toimivia molemmissa, joten jos ei erityistarpeita ole, niin samat asetukset voidaan laittaa myös reaaliaikaiselle skannerille. Ainoa ero on mahdollisuus myös monitoroida verkkokiintolevyjä. Tämä kuitenkin voidaan jättää pois päältä, jos sille ei uskota olevan tarvetta.

Update kohdassa päätetään, kuinka usein Aviran viruksentorjuntaohjelmisto päivitetään. Jos yritys käyttää välityspalvelinta, niin plus-merkkiä painamalla päästään määrittelemään niiden asetukset **Web server**in alta löytyvästä **Proxy settings** kohdasta.

Viruksentorjuntaohjelmistot on pidettävä aina ajantasalla ja niihin on saatava päivitykset heti, kun mahdollista. Aviran ilmaisessa viruksentorjuntaversiossa kuitenkin voi määritellä minimiksi 6 tuntia, joten se on suositeltavaa laittaa. Maksullisissa viruksentorjuntaohjelmistoissa yleensä käyttäjä saa ilmoituksen, kun uudet päivitykset on julkaistu jolloin ne saadaan samantien ladattua.

8.2 Palomuurin asetukset

Palomuurin asetukset ovat oletuksena niin, että kaikki liikenne estetään. Käyttäjän tehtävänä on määritellä, mitkä ohjelmat saavat käyttää verkkoliikennettä. Esimerkissä käydään läpi Comodo Firewallin asetuksia, mutta toimintaperiaate on kaikissa palomuureissa sama. Kuvio 9:stä selviää palomuurin asetuksia ja niitä käydään alla läpi.



Kuvio 9. Palomuurin asetuksien määrittely Comodo Firewallissa.

Allow Application kohdasta voidaan määritellä ohjelmat, joiden verkkoliikenne päästetään palomuurin läpi. Vain luotettavat ohjelmat tulisi sallia.

Block Application estää verkkoliikenteen ohjelmilta.

Stealth Ports antaa estää kaikki tulevan liikenteen, jolloin tietokone on "näkymätön" muille tietokoneille. Toinen vaihtoehto on antaa ilmoitus aina tulevasta yhteydestä, jolloin pystytään päättämään erikseen jokaisen yhteyden kohdalla, annetaanko sille lupa nähdä tietokone vai ei.

Manage Networks kohdasta voidaan sallia tai estää sisäverkon yhteyksiä.

Stop Newtwork Activitystä pystytään estämään kaikki sisään tai ulos menevä verkkoliikenne

Open Advanced Settings avaa ikkunan, josta päästään määrittelemään muita palomuurin asetuksia, kuten yksityisten verkkojen automaattisen tunnistamisen ja graafisen käyttöliittymän asetuksia.

9 Tietoturvan tila yrityksessä

Tietoturvan tarkastamiseen on erilaisia keinoja mutta ulkopuolisille ei kuitenkaan saisi antaa mitään tietoa yrityksen tietoturvasta. Hyökkääjät pystyvät käyttämään tietoja hyväksi, joten tulee aina noudattaa varovaisuuttaa tietoturvasta puhuttaessa. Erilaisia tietoturvakyselyitä tehdessä on hyvä varmistaa, että tiedot menevät luotettavalle taholle.

Tämän työn liitteeksi on tehty lyhyt kysely, jonka täyttämällä pystytään saamaan jonkinlaista kuvaa oman yrityksen tietoturvan tilasta. Kysely on ainoastaan yrityksen omaan käyttöön, eikä sitä tule näyttää tai lähettää ulkopuolisille. Vaihtoehtoja voi valita useita yhdessä kysymyksessä. Nyrkkisääntönä voidaan pitää, että mitä useampia kohtia tulee valittua, sen paremmassa kunnossa tietoturva on. Kyselyssä voi kuitenkin olla myös vaihtoehtoja, jotka eivät lisää jokaisen yrityksen tietoturvaa, joten kysely on vain suuntaa antava.

10 Opinnäytetyön pohdinta

Opinnäytetyössä tavoiteltiin sitä, että tehdään pienille ja keskisuurille yrityksille opas, joka sisältää yleisesti tietoa tietoturvasta ja tavoitteeseen päästiin. Ohjeet pystytään luokittelemaan luotettaviksi, koska tiedot on haettu luotettavista lähteistä, kuten eri yliopistojen nettisivuilta, tutkimustuloksista, tietoturvayhtiöiltä, ohjelmistovalmistajilta ja alan ammttilaisilta.

Kehittyminen

Opinnäytetyön tekemisen aikana tuli opittua paljon uutta tietoturvasta. Yrityksen kannalta tietoturvan pohtiminen oli erittäin kiinnostavaa, sillä silloin täytyi ottaa huomioon erilaiset tarpeet ja selvittää paras mahdollinen keino täyttää nämä tarpeet.

Haasteet

Haasteena oli kaikkien pienten ja keskisuurten yrityksien tarpeiden huomioon ottaminen opasta tehdessä. Tiedot tuli saada kirjoitettua niin selkeäksi, että kuka vain pystyy ymmärtämään oppaan sisällön. Opasta ei ollut kohdennettu mitenkään tiettyyn yritykseen vaan yleisesti kaikkiin pk-yrityksiin, joten oppaassa tuli ottaa kaikki mahdolliset yrityksiin kohdistuvat uhat huomioon.

Ongelmat

Opinnäytetyön tekemisen aikana ei ilmennyt suurempia vastoinkäymisiä. Ajanhallintaan olisi pitänyt panostaa enemmän ja välillä tuntui, että tulee hieman kiire mutta loppujen lopuksi aikataulussa pysyttiin hyvin. Välillä ongelmia aiheuttivat väärät tiedot, joita saatiin epäluotettavista lähteistä.

Lähteet

Acronis. Luettavissa:
http://www.acronis.com/en-us/resource/solutions/backup/2005/incremental-backups.html. Luettu 3.3.2014.

Chris Hoffman 2013. How-To Geek. Why You Don't Need to Install a Third-Party Firewall (And When You Do)
Luettavissa: http://www.howtogeek.com/165203/why-you-dont-need-to-install-a-third-party-firewall-and-when-you-do/. Luettu 16.1.2014

Daniel Soper 2013. Introduction to Computer Security.
Luettavissa: www.youtube.com/watch?v=zBFB34YGK1U. Luettu 23.1.2014

David Howell 2012. techradar. How to choose an uninterruptable power supply for your business. Luettavissa: http://www.techradar.com/news/world-of-tech/roundup/how-to-choose-an-uninterruptable-power-supply-for-your-business-1113542. Luettu 3.3.2014

Düperthal Luettavissa:
http://www.dueperthal.de/data/oxid.php/sid/9adf6001925a15f704b7d8a1cbb01ca2/cl/content/tpl/7134de38a3e5a5328.56188905/lang/1. Luettu 21.1.2014

EmersonNetworkPower. Avoidin Trap Doors, s. 3. Luettavissa:
http://www.emersonnetworkpower.com/en-US/Brands/Liebert/Documents/White%20Papers/UPS%20Trap%20Doors%20for%20SMB.PDF. Luettu 20.1.2014

F-secure. Luettavissa: http://www.f-secure.com/v-descs/backdoor.shtml. Luettu 1.2.2014

Griffith University. Average computer energy usage. Luettavissa: http://www.griffith.edu.au/sustainability/sustainable-campuses/sustainable-initiatives/energy/average-computer-energy-usage. Luettu 7.3.2014

Juha Tuppi, 2013. Hardware. Luettavissa: http://www.hardware.fi/uutiset/artikkeli.cfm/2013/11/13/kovalevyjen_elinkaarta_selvitetty_25_000_kovalevyn_perusteella. Luettu 7.3.2014

Kari Kemppainen 2005. Digitoday. Tietoturvan ulkoistus tehtävä harkiten. Luettavissa: http://www.digitoday.fi/tietoturva/2005/09/16/tietoturvan-ulkoistus-tehtava-harkiten/200515261/66. Luettu 21.2.2014

Katherine Noyes 2010. Why Linux is More Secure Than Windows. Luettavissa: http://www.pcworld.com/article/202452/why_linux_is_more_secure_than_windows.html. Luettu: 14.1.2014.

Kauppa- ja teollisuusministeriö, PK-yritysten tietoturvakysely 2006 Luettavissa: http://www.ek.fi/ek/fi/yrittajyys_ym/yrittajyys/tietoa_pk-yrityksista/liitteet/Pk-yritystentietoturvakysely.pdf. Luettu 22.1.2014

Lance Spitzner 2003. Tracking Hackers – Honeypots. Luettavissa: http://www.tracking-hackers.com/papers/honeypots.html. Luettu 28.1.2014

Margaret Rouse 2008. SearchMidmarketSecurity. Luettavissa: http://searchmidmarketsecurity.techtarget.com/definition/rootkit. Luettu 19.3.2014

Mary Landesman. About.com - Antivirus Software. Luettavissa: http://antivirus.about.com/od/spywareandadware/a/adware.htm. Luettu 2.2.2014

Microsoft. Malware Protection Center. Luettavissa: https://www.microsoft.com/security/portal/mmpc/threat/exploits.aspx. Luettu 1.2.2014

Symantec a - Viruses that can cost you
Luettavissa: http://www.symantec.com/region/reg_eu/resources/virus_cost.html. Luettu: 14.1.2014

Symantec b - Worms
Luettavissa:
http://www.symantec.com/security_response/glossary/define.jsp?letter=w&word=worms. Luettu: 14.1.2014

Symantec c - Trojan horse
Luettavissa: http://www.symantec.com/security_response/writeup.jsp?docid=2004-021914-2822-99. Luettu 15.1.2014

Types of Backup. Luettavissa: http://typesofbackup.com/. Luettu 29.1.2014

United States Computer Emergency Readiness Team
Luettavissa: http://www.us-cert.gov/publications/virus-basics#email. Luettu: 14.1.2014

UTU. UPS-laitteet tulppaliitännällä. Luettavissa:
http://www.utu.eu/tuotteet/tietoliikenne-ja-turvatuotteet/ups-laitteet-ja-muuntajat/ups-laitteet-tulppaliitannalla. Luettu: 3.3.2014

Valtiovarainministeriö 2003. Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa. Valtionhallinnin tietoturvallisuuden johtoryhmä. Vahti, s. 31–32. Luettavissa:
http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/53828/53827_fi.pdf. Luettu 27.3.2014.

webopedia 2007. The Differences Between WEP and WPA. Luettavissa:
http://www.webopedia.com/DidYouKnow/Computer_Science/WEP_WPA_wireless_security.asp. Luettu 6.2.2014.

webopedia 2010. The Differences and Features of Hardware and Software Firewalls. Luettavissa: http://www.webopedia.com/DidYouKnow/Hardware_Software/firewall_types.asp. Luettu 21.2.2014.

Liitteet

Liite 1. Tietoturvakysely yritykselle 1/2

1. Onko yrityksellänne ajantasalla oleva viruksentorjuntaohjelmisto?

[ ] Kyllä [ ] Ei [ ] En osaa sanoa

2. Minkälaisia palomuuriratkaisuja yrityksellänne on?

[ ] Ohjelmallinen palomuuri

[ ] Rautapalomuuri

[ ] Tilaton palomuuri

[ ] Tilallinen palomuuri

[ ] Yrityksessä ei ole palomuuria käytössä

[ ] En osaa sanoa

3. Onko yrityksenne ohjelmistot päivitettynä ajantasalle?

[ ] Kyllä [ ] Ei [ ] En osaa sanoa

4. Ovatko yrityksen laitteiden käyttöjärjestelmät päivitetty ajantasalle?

[ ] Kyllä [ ] Ei [ ] En osaa sanoa

5. Onko henkilökunta perehdytetty

[ ] työskentelemään tietoturvallisesti?

[ ] käyttämään varmuuskopiointia?

[ ] käyttämään ja säilyttämään siirrettäviä medioita oikeaoppisesti?

[ ] käsittelemään arkaluontoista tietoa?

[ ] käyttämään turvallisia salasanoja?

[ ] käyttämään sähköpostia?

[ ] hävittämään dokumentit asianmukaisin keinoin?

Liite 2. Tietoturvakysely yritykselle 2/2

6. Ovatko yrityksen laitteistot

[ ] suojattu UPS laitteistoilla?

[ ] suljetussa tilassa/lukittu esim. vaijerilukolla?

7. Ovatko yrityksen tiedot

[ ] Varmuuskopioitu?

[ ] salattu kryptaamalla?

8. Onko yrityksen langaton verkko suojattu?

[ ] Kyllä, WEP salauksella

[ ] Kyllä, WPA salauksella

[ ] Ei

[ ] Yrityksessä ei käytetä langatonta verkkoa

9. Mahdollisiin hyökkäyksiin on varauduttu

[ ] Hunajapurkilla

[ ] Lieventämällä hyökkäyksen aiheuttamia tuhoja

[ ] Hyökkäyksestä nopealla palautumisella

10. Yrityksen varmuuskopiointi on hoidettu

[ ] Siirrettävillä medioilla (cd- ja dvd-levyt, muistitikut, ulkoinen kovalevy)

[ ] Toisilla kovalevyillä

[ ] Yrityksen omalla palvelimella

[ ] Nauha-asemalla

[ ] Pilvipalveluissa

11. Onko yrityksen tietoturva ulkoistettu?

[ ] Kyllä [ ] Ei